FORTINET

Virtual FortiOS - Admin Guide

Version 5.6

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

Thursday, April 26, 2018

FortiOS™ Handbook - VM Installation

01-560-203906-20180124

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-01-19	• Added information about other Virtual FortiOS Products • Handbook name change.
2018-01-09	• Added CLI info on license installation. Changed screen shot for VM license upload. • Addition information added about license status.
2017-11-10	Adjustment in min/max memory for FG-VM00
2017-10-26	Added information on Licensing timeout
2016-10-31	Initial Release.

Introduction

FortiGate virtual appliances allow you to mitigate blind spots by implementing critical security controls within your virtual infrastructure. They also allow you to rapidly provision security infrastructure whenever and wherever it is needed. FortiGate virtual appliances feature all of the security and networking services common to traditional hardware-based FortiGate appliances. With the addition of virtual appliances from Fortinet, you can deploy a mix of hardware and virtual appliances, operating together and managed from a common centralized management platform.

Document scope

This document describes how to deploy a FortiGate virtual appliance in several virtualization server environments. This includes how to configure the virtual hardware settings of the virtual appliance.

This document assumes:

- you have already successfully installed the virtualization server on the physical machine,
- you have installed appropriate VM management software on either the physical server or a computer to be used for VM management.

This document does not cover configuration and operation of the virtual appliance after it has been successfully installed and started. For these issues, see the FortiGate Handbook.

This document includes the following sections:

What's new in VM in 5.6

New Features in 5.6.4

The following list contains new virtual FortiOS features added in FortiOS 5.6.4. Click on a link to navigate to that section for further information.

- FortiGate VMX license status
- SDN connector addressing on page 18
- Support for KVM-based hypervisor in AWS on page 19
- HA support for GCP on page 22
- HA support for Azure on page 20

FortiGate VMX licence status

The VMX licence status is included in the output of `get system status`.

SDN connector addressing

When setting the address for an SDN connection, the value can be a fully qualified domain name (FQDN) as well as an IP address. The setting that is currently called `server` was once called `server-ip`.

Support for KVM-based hypervisor in AWS

FortiGate-VM can be provisioned in AWS C5 instances on the marketplace (BYOL/OnDemand). These instances are based on a home-brewed version of KVM that AWS started using. Systems deployed in C5 will see better performance compared to C3/C4 instances. Deploying FortiGate-VM in these instances requires no configuration on the part of the user.

HA support for GCP

FortiOS supports the use of active/passive HA, using a unicast heartbeat, in Google Cloud Platform (GCP) similar to the HA support for Amazon Web Services (AWS).

HA support for Azure

FortiOS supports the use of active/passive HA, similar to that for Amazon Web Services (AWS) in an Azure environment.

New Features in 5.6.0

FGT-VM VCPUs (308297)

Fortinet has now launched licensing for FortiGate VMs that support larger than 8 vCPUs. The new models/licenses include:

- Support for up to 16 vCPU - FortiGate-VM16
- Support for up to 32 vCPU - FortiGate-VM32
- Support for unlimited vCPU - FortiGate-VMUL

Each of these models should be able to support up to 500 VDOMs.

Improvements to License page (382128)

The page has been rewritten with some minor improvements such as:

- An indicator to show when a VM is waiting for authentication or starting up
- Shows VM status when license is valid
- Shows CLI console window when VM is waiting too long for remote registration of server

Citrix XenServer tools support for XenServer VMs (387984)

This support allows users, with Citrix XenServer tools to read performance statistics from XenServer clients and do Xenmotion with servers in the same cluster

Since FortiGates don't support hardware hotplugging, the ability to do network interface of disk changes is not supported at this time.

There are no changes to the GUI, but there are some changes to the CLI.

A setting has been edited to control the debug level of the XenServer tools daemon

```
diag debug application xstoolsd <integer>
```

Integer = Debug level

An additional update has been added to set the update frequency for XenServer tools

```
config system global
   set xstools-update-frequency Xenserver <integer>
   end
```

Enter an integer value from `30` to `300` (default = 60).

FOS VM supports more interfaces (393068)

The number of virtual interfaces that the VM version of FortiOS supports has been raised from 3 to 10.

NSX security group importing (403975)

A feature has been added to allow the importation of security group information from VMware's NSX firewall.

CLI Changes:

nsx group list

This is used to list NSX security Groups

Syntax:

```
execute nsx group list <name of the filter>
```

nsx group import

This is used to import NSX security groups.

Syntax:

```
execute nsx group import <vdom> <name of the filter>
```

nsx group delete

This is used to delete NSX security Groups

Syntax:

```
execute nsx group delete <vdom> <name of the filter>
```

nsx.setting.update-period

This is used to set the update period for the NSX security group

Syntax:

```
config.nsx.setting.update-period <0 - 3600 in seconds>
```

`0` means disabled

Default value: `0`

Non-vdom VM models FGVM1V/FGVM2V/FGVM4V (405549)

New models of the FortiGate-VM have been introduced. These match up with the existing FortiGate-VM models of FG-VM01, FG-VM02 and FG-VM04. The difference being that the new models don't support VDOMs.

Original FortiGate-VM	New FortiGate-VM without VDOM support
FG-VM01	FG-VM01v

Original FortiGate-VM	New FortiGate-VM without VDOM support
FG-VM02	FG-VM02v
FG-VM04	FG-VM04v

Virtual FortiOS Overview

The following topics are included in this section:

FortiGate VM models and licensing

Fortinet offers the FortiGate VM in five virtual appliance models determined by license. When configuring your FortiGate VM, be sure to configure hardware settings within the ranges outlined below. Contact your Fortinet Authorized Reseller for more information.

FortiGate VM model information

Technical Specification	FG-VM00	FG-VM01	FG-VM02	FG-VM04	FG-VM08
Virtual CPUs (min / max)	1 / 1	1 / 1	1 / 2	1 / 4	1 / 8
Virtual Network Interfaces (min / max)			2 / 10		
Virtual Memory (min / max)	1GB / 2GB	1GB / 2GB	1GB / 4GB	1GB / 6GB	1GB /12GB
Virtual Storage (min / max)			32GB / 2TB		
Managed Wireless APs (tunnel mode / global)	32 / 32	32 / 64	256 / 512	256 / 512	1024 / 4096
Virtual Domains (default / max)	1 / 2	10 / 10	10 / 25	10 / 50	10 / 250

There may be times the min/max values can change. An example for this is when the maximum memory for FG-VM00 changed between 5.2 and 5.4 from 1 GB to 1.5 GM. If that is the case, the settings for the VM will have to be manually changed to accommodate the new parameters.

After placing an order for FortiGate VM, a license registration code is sent to the email address used on the order form. Use the registration number provided to register the FortiGate VM with Customer Service & Support and then download the license file. Once the license file is uploaded to the FortiGate VM and validated, your FortiGate VM appliance is fully functional.

The number of Virtual Network Interfaces is not solely dependent on the FortiGate VM. Some virtual environments have their own limitations on the number of interfaces allowed. As an example, if you go to https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-multiple-nics, you will find that Azure has its own restrictions for VMs, depending on the type of deployment or even the size of the VM.

FortiGate VM evaluation license

FortiGate VM includes a limited embedded 15-day trial license that supports:

- 1 CPU maximum
- 1024 MB memory maximum
- low encryption only (no HTTPS administrative access)
- all features except FortiGuard updates

You cannot upgrade the firmware, doing so will lock the Web-based Manager until a license is uploaded. Technical support is not included. The trial period begins the first time you start FortiGate VM. After the trial license expires, functionality is disabled until you upload a license file.

Registering FortiGate VM with Customer Service & Support

To obtain the FortiGate VM license file you must first register your FortiGate VM with Customer Service & Support.

To register your FortiGate VM:

1. Log in to the Customer Service & Support portal using an existing support account or select **Sign Up** to create a new account.
2. In the main page, under **Asset**, select **Register/Renew**.

   The **Registration** page opens.
3. Enter the registration code that was emailed to you and select **Register**. A registration form will display.
4. After completing the form, a registration acknowledgement page will appear.
5. Select the **License File Download** link.
6. You will be prompted to save the license file (`.lic`) to your local computer. See "Upload the license file" for instructions on uploading the license file to your FortiGate VM via the Web-based Manager.

Downloading the FortiGate VM deployment package

FortiGate VM deployment packages are included with FortiGate firmware images on the Customer Service & Support site. First, see the following table to determine the appropriate VM deployment package for your VM platform.

Selecting the correct FortiGate VM deployment package for your VM platform

VM Platform	FortiGate VM Deployment File
Citrix XenServer v5.6sp2, 6.0 and later	FGT_VM64-v500-buildnnnn-FORTINET.out.CitrixXen.zip
OpenXen v3.4.3, 4.1	FGT_VM64-v500-buildnnnn-FORTINET.out.OpenXen.zip
Microsoft Hyper-V Server 2008R2 and 2012	FGT_VM64-v500-buildnnnn-FORTINET.out.hyperv.zip
KVM (qemu 0.12.1)	FGT_VM64-v500-buildnnnn-FORTINET.out.kvm.zip
VMware ESX 4.0, 4.1 ESXi 4.0/4.1/5.0/5.1/5.5	FGT_VM32-v500-buildnnnn-FORTINET.out.ovf.zip (32-bit) FGT_VM64-v500-buildnnnn-FORTINET.out.ovf.zip

For more information see the FortiGate product datasheet available on the Fortinet web site, http://www.fortinet.com/products/fortigate/virtualappliances.html.

The firmware images FTP directory is organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention and each firmware image is specific to the device model. For example, the FGT_VM32-v500-build0151-FORTINET.out.ovf.zip image found in the v5.0 Patch Release 2 directory is specific to the FortiGate VM 32-bit environment.

You can also download the FortiOS Release Notes, FORTINET-FORTIGATE MIB file, FSSO images, and SSL VPN client in this directory. The Fortinet Core MIB file is located in the main FortiGate v5.00 directory.

To download the FortiGate VM deployment package:

1. In the main page of the Customer Service & Support site, select **Download** > **Firmware Images**.

   The **Firmware Images** page opens.
2. In the **Firmware Images** page, select **FortiGate**.
3. Browse to the appropriate directory on the FTP site for the version that you would like to download.

4. Download the appropriate `.zip` file for your VM server platform.

   You can also download the FortiGate Release Notes.
5. Extract the contents of the deployment package to a new file folder.

Deployment package contents

Citrix XenServer

The FORTINET.out.CitrixXen.zip file contains:

- fortios.vhd: the FortiGate VM system hard disk in VHD format
- fortios.xva: binary file containing virtual hardware configuration settings
- in the ovf folder:
  - FortiGate-VM64.ovf: Open Virtualization Format (OVF) template file, containing virtual hardware settings for Xen
  - fortios.vmdk: the FortiGate VM system hard disk in VMDK format
  - datadrive.vmdk: the FortiGate VM log disk in VMDK format

The ovf folder and its contents is an alternative method of installation to the .xva and VHD disk image.

OpenXEN

The FORTINET.out.OpenXen.zip file contains only fortios.qcow2, the FortiGate VM system hard disk in qcow2 format. You will need to manually:

- create a 32GB log disk
- specify the virtual hardware settings

Microsoft Hyper-V

The FORTINET.out.hyperv.zip file contains:

- in the Virtual Hard Disks folder:
  - fortios.vhd: the FortiGate VM system hard disk in VHD format
  - DATADRIVE.vhd: the FortiGate VM log disk in VHD format
- In the Virtual Machines folder:
  - fortios.xml: XML file containing virtual hardware configuration settings for Hyper-V. This is compatible with Windows Server 2012.
- Snapshots folder: optionally, Hyper-V stores snapshots of the FortiGate VM state here

KVM

The FORTINET.out.kvm.zip contains only fortios.qcow2, the FortiGate VM system hard disk in qcow2 format. You will need to manually:

- create a 32GB log disk
- specify the virtual hardware settings

VMware ESX/ESXi

You will need to create a 32GB log disk.

The FORTINET.out.ovf.zip file contains:

- fortios.vmdk: the FortiGate VM system hard disk in VMDK format
- datadrive.vmdk: the FortiGate VM log disk in VMDK format
- Open Virtualization Format (OVF) template files:
  - FortiGate-VM64.ovf: OVF template based on Intel e1000 NIC driver
  - FortiGate-VM64.hw04.ovf: OVF template file for older (v3.5) VMware ESX server
  - FortiGate-VMxx.hw07_vmxnet2.ovf: OVF template file for VMware vmxnet2 driver
  - FortiGate-VMxx.hw07_vmxnet3.ovf: OVF template file for VMware vmxnet3 driver

Use the VMXNET3 interface (FortiGate-VMxx.hw07_vmxnet3.ovf template) if the virtual appliance will distribute workload to multiple processor cores.

Deploying the FortiGate VM appliance

Prior to deploying the FortiGate VM appliance, the VM platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for FortiGate VM assume that

- You are familiar with the management software and terminology of your VM platform.
- An Internet connection is available for FortiGate VM to contact FortiGuard to validate its license or, for closed environments, a FortiManager can be contacted to validate the FortiGate VM license. See "Validate the FortiGate VM license with FortiManager".

For assistance in deploying FortiGate VM, refer to the deployment chapter in this guide that corresponds to your VMware environment. You might also need to refer to the documentation provided with your VM server. The deployment chapters are presented as examples because for any particular VM server there are multiple ways to create a virtual machine. There are command line tools, APIs, and even alternative graphical user interface tools.

Before you start your FortiGate VM appliance for the first time, you might need to adjust virtual disk sizes and networking settings. The first time you start FortiGate VM, you will have access only through the console window of your VM server environment. After you configure one FortiGate network interface with an IP address and administrative access, you can access the FortiGate VM web-based manager.

After deployment and license validation, you can upgrade your FortiGate VM appliance's firmware by downloading either FGT_VM32-v500-buildnnnn-FORTINET.out (32-bit) or FGT_VM64-v500-buildnnnn-FORTINET.out (64-bit) firmware. Firmware upgrading on a VM is very similar to upgrading firmware on a hardware FortiGate unit.

FortiGate-VM is not part of the FortiGuard Network for the purpose of upgrades.

Performance and optimization

Performance is improved for FortiOS VM platforms by implementing features to improve efficiency and resource utilization.

Interrupt affinity

You can configure interrupt affinity and packet distribution to optimize performance for your VM environment. Interrupt affinity allows you to align interrupts from interfaces to specific CPUs.

Configuring interrupt affinity

Use the following commands to configure interrupt affinity for two 10G interfaces (port2 and port3).

Interrupts from first interface are assigned to core #0 and those from the second interface are assigned to core #1.

```
config system affinity-interrupt
   edit 1
      set interrupt "port2-TxRx-0"
      set affinity-cpumask "0x1"
   next
   edit 2
      set interrupt "port2-TxRx-1"
      set affinity-cpumask "0x1"
   next
   edit 3
      set interrupt "port3-TxRx-0"
      set affinity-cpumask "0x2"
   next
   edit 4
      set interrupt "port3-TxRx-1"
      set affinity-cpumask "0x2"
   end
```

Packet distribution

Packet distribution allows you to configure FortiGate-VM to distribute processing to multiple CPUs.Use the following commands to configure packet redistribution to redistribute packets from core #0 and #1 to all other cores.

Configuring packet distribution

The example is based on VM08:

```
config system affinity-packet-redistribution
   edit 1
      set interface "port2"
      set affinity-cpumask "0xFC"
   next
   edit 2
      set interface "port3"
      set affinity-cpumask "0xFC"
   end
```

Other Virtual FortiOS Products

Just like a VM installed on a platform located on a physical computer, these are instances of the FortiOS firmware installed in virtual environments.

SDN Environments

FortiOS-VM is now supported in a Number of SDN (Software Defined Network) environments through the use of a SDN connector. The software can be found on the Fortinet Service and Support site. Documentation can be found on the Fortinet Documentation site under the product heading of Fortinet Connectors.

The products include:

FortiGate-VMX

Admin guide can be found at https://docs.fortinet.com/d/fortigate-vmx-install-v.2.

FortiOS On Demand

Admin guide can be found at https://docs.fortinet.com/d/fortigate-fortinetvm-on-demand-administration-guide.

Connectors:

The SDN connectors provide integration and orchestration of Fortinet products with key SDN solutions. Fortinet provides SDN connector support for public cloud connectors, such as VMware NSX, Cisco Application Centric Infrastructure (ACI), and Nokia Nuage Virtualized Services Platform (VSP) . Fortinet also provides support for private cloud connectors, such as Amazon Web Services and Microsoft Azure. You can configure SDN connectors in the **System > SDN Connectors** menu.

Microsoft Azure only supports tag sets in Virtual Machines (VMs). You may only use one Azure subscription ID and one Azure resource group. Only resources that are in use by a running VM, such as a virtual network, subnet, or network security group, are extracted.

FortiADC Connector for Cisco ACI

- Guides found at https://docs.fortinet.com/fortinet-connectors/admin-guides.
- Versions available:
  - 1.0.0
  - 1.2.0
  - 1.3.0

FortiADC Connector for Cisco ACI

- Guides found at https://docs.fortinet.com/fortinet-connectors/admin-guides.
- Versions available:
  - 1.0.0
  - 1.2.0
  - 1.3.0

FortiGate Connector for HPE VAN SDN

- Guides found at https://docs.fortinet.com/fortinet-connectors/admin-guides.
- Versions available:
  - 1.0.5
  - 1.1.0

FortiGate Connector for OpenStack ML2

- Guides found at https://docs.fortinet.com/fortinet-connectors/admin-guides.
- Versions available:
  - 1.1

FortiManager Connector for Nuage Networks

- Guides found at https://docs.fortinet.com/fortinet-connectors/admin-guides.
- Versions available:
  - 1.0

Fortinet SDN Connector for Nuage VSP

Instruction can be found at http://cookbook.fortinet.com/nuage-vsp/

Additional information relating to Connectors

While the product documentation concerns itself with the connector software, there is also settings within FortiOS that relates to the usage of those connectors.

NSX Connector Support

There is support for NSX connector to upgrade to SDN connectors.

Change to `config system sdn-connector`:

```
config nsx setting
```

Change to `config firewall address`:

```
set type nsx

set type dynamic
   set sdn nsx
```

When using the sdn nsx setting, the user should also use the nsx rest-api password.

SDN connector addressing

When setting the address for an SDN connection, the value can be a fully qualified domain name (FQDN) as well as an IP address. The setting that is currently called `server` was once called `server-ip`.

CLI

```
config system sdn-connector
   edit <example>
      set server [<ip address>|<fqdn address>]
```

```
end
```

Public Cloud Environments

Unlike SDNs where the user has administrative control over he virtual environment that the FortiOS is being placed into, the Public Cloud services are run and managed by 3rd party companies with their own methods and rules of provisioning that need to be followed to install the firmware into the environment.

Amazon Web Services (AWS)

Online documentation can be found at http://cookbook.fortinet.com/amazon-web-services-aws/

Additional information for AWS

While the online documentation is primarily for the installation of the FortiOS into the virtual environment, periodically improvements are made to the firmware that affects its interaction with the environment but isn't really covered by installation instructions or information has changed in regards to those instructions but they may not have all been updated yet.

Support for KVM-based hypervisor in AWS

FortiGate-VM can be provisioned in AWS C5 instances on the marketplace (BYOL/OnDemand). These instances are based on a home-brewed version of KVM that AWS started using. Systems deployed in C5 will see better performance compared to C3/C4 instances. Deploying FortiGate-VM in these instances requires no configuration on the part of the user.

FortiGate-VM firmware can be placed in these instances because of:

- An NVME driver that is required to run C5 instances. It gets the correct partition name dependencies if an NVME device is being used.
- Removing the `xenstore` checking requirement in the AWS setup daemon that is not required in non-Xen based instances.

HA

AWS supports the use of HA.

This includes two parts:

1. HA with unicast heartbeat traffic.
2. AWS API supports to move secondary IPs and update routing tables.

   CLI:

   Unicast HA config

```
config system ha
   unicast-hb [enable|disable]
   unicast-hb-peerip <Unicast Heartbeat Peer IP>
   end
```

SDN Connector - AWS

SDN connectors can be configured in the GUI by going to **System > SDN Connectors** and choosing the appropriate type to configure from the various virtual environments. AWS is supported in the GUI as well as the CLI.

1. `config aws setting` has been moved to the context of `config system sdn-connector`.
```
config system sdn-connector
   edit <string>
      set access-key <AWS access key ID>
      set secret-key <AWS secret access key>
      set region <AWS region name>
      set vpc-id <AWS VPC ID>
      end
```
2. Update to the GUI SDN connector edit page that supports allowing configuration of the following fields:
   - AWS access key ID
   - AWS secret access key
   - AWS region name
   - AWS VPC ID
   - Update Interval
3. Change to address edit page to allow configuration of the **Filter** field for Dynamic AWS address.
4. Update to the dynamic address monitor API to get resolved address list for dynamic AWS addresses.

Azure

HA support for Azure

FortiOS supports the use of active/passive HA, similar to that for Amazon Web Services (AWS) in an Azure environment.

SDN Connector - Azure

SDN connectors can be configured in the GUI by going to **System > SDN Connectors** and choosing the appropriate type to configure from the various virtual environments. Azure is supported in the GUI as well as the CLI.

CLI options are available to configure with Azure:

- The `system sdn-connector` contains a connector type for Azure environments called `azure`.
- The `nic` option enables you to configure the Azure network interface.
- The `route-table` option enables you to configure the Azure route table.

Example:

```
config system sdn-connector
   edit "azd"
      set type azure
      config nic
         edit nic-eth2
            config ip
               edit ipconfig1
                  set public-ip p3
               next
            end
         next
         edit nic-eth3
            config ip
               edit ipconfig1
                  set public-ip p2
               next
```

```
        end
    next
end
config route-table
    edit 1
        config route
            edit 12
                set next-hop 111.233.222.233
            next
        end
    next
end
```

In addition to the options for HA already specified, there are settings specific to Azure connectivity within the `system sdn-connector` context once the `type` has been set to `azure`.

Option	Description
tenant-id	Azure tenant ID (directory ID).
subscription-id	Azure subscription ID.
client-id	Azure client ID (application ID).
client-secret	Azure client secret (application key).
resource-group	Azure resource group.
azure-region	Global/China Azure Region.
update-interval	Dynamic object update interval in seconds (`0 - 3600`, `0` means disabled, default = `60`).

Online documentation can be found at http://cookbook.fortinet.com/microsoft-azure/

Google Cloud Platform (GCP)

The following FortiGate-VM models will be supported on Google Cloud Platform:

- FG-VM01
- FG-VM02
- FG-VM04
- FG-VM08

FG-WM00 is not supported.

Since GCP use netmask 32, static route must be configured on GCP VPC, instead of FGT.

Licenses will be interchangeable between platforms. A FG-VM04 license that functions in a VMware or Citrix environment can be also used in the GCP environment as well.

While an .out file will be necessary for upgrading, full downloadable images will not be needed for initial installation of the solution. GCP consists of pre-existing images that can be checked out of their library and deployed instantly. A difference between this environment and enterprise virtualization platforms is that machine size can never change. An n1-standard-4 has exactly 15 GB of RAM and 4 vCPUs. This can never be changed or edited by the end user or administrator.

The currently available GCP instances we are looking to support are as follows (these will/could change as vNIC values reveal themselves):

FG-VM	Equates to Instance Type	vCPU	RAM	Disks
FG-VM01-GC	n1-standard-1	1	3.75GB	16 (32 in Beta)
FG-VM02-GC	n1-standard-2	2	7.50 GB	16 (64 in Beta)
FG-VM04-GC	n1-standard-4	4	15 GB	16 (64 in Beta)
FG-VM08-GC	n1-standard-8	8	30 GB	16 (128 in Beta)
FG-VM16-GC	n1-standard-16	16	60 GB	16 (128 in Beta)
FG-VM32-GC	n1-standard-32	32	88 GB	16 (128 in Beta)
FG-VMUL-GC	any of the above and any new that could be created.			

HA support for GCP

FortiOS supports the use of active/passive HA, using a unicast heartbeat, in Google Cloud Platform (GCP) similar to the HA support for Amazon Web Services (AWS).

This support includes:

- HA in the same region within a project
- HA session and configuration synchronization
- Automatic failover to the passive unit (time dependant on configuration), using the built-in API call to GCP for changing the routing path from the active unit to the passive unit.

There is a new connector type, `gcp`, that has been added to the `type` option for `system sdn-connector` as well as a setting for the mask of the unicast heartbeat in `system ha`.

GCP type example:

```
config system sdn-connector
   edit gcp
      set type gcp
      config external-ip
         edit gundam-public
         next
      end
      config route
         edit gundam-route
         next
```

```
      end
   next
end
```

Unicast example:

```
config system ha
   set group-id 20
   set group-name "cluster1"
   set mode a-p
   set hbdev "port3" 50
   set ha-mgmt-status enable
   config ha-mgmt-interfaces
      edit 1
         set interface "port4"
         set gateway 172.16.100.1
      next
   end
   set override disable
   set priority 20
   set unicast-hb enable
   set unicast-hb-peerip 172.16.201.3
   set unicast-hb-netmask 255.255.255.0
end
```

Additional information from GCP: https://cloud.google.com/compute/docs/images/building-custom-os.

Deployment example – VMware

Once you have downloaded the FGT_VMxx-v5-build0xxx-FORTINET.out.ovf.zip file from http://support.fortinet.com and extracted the package contents to a folder on your local computer, you can use the vSphere client to create the virtual machine from the deployment package OVF template.

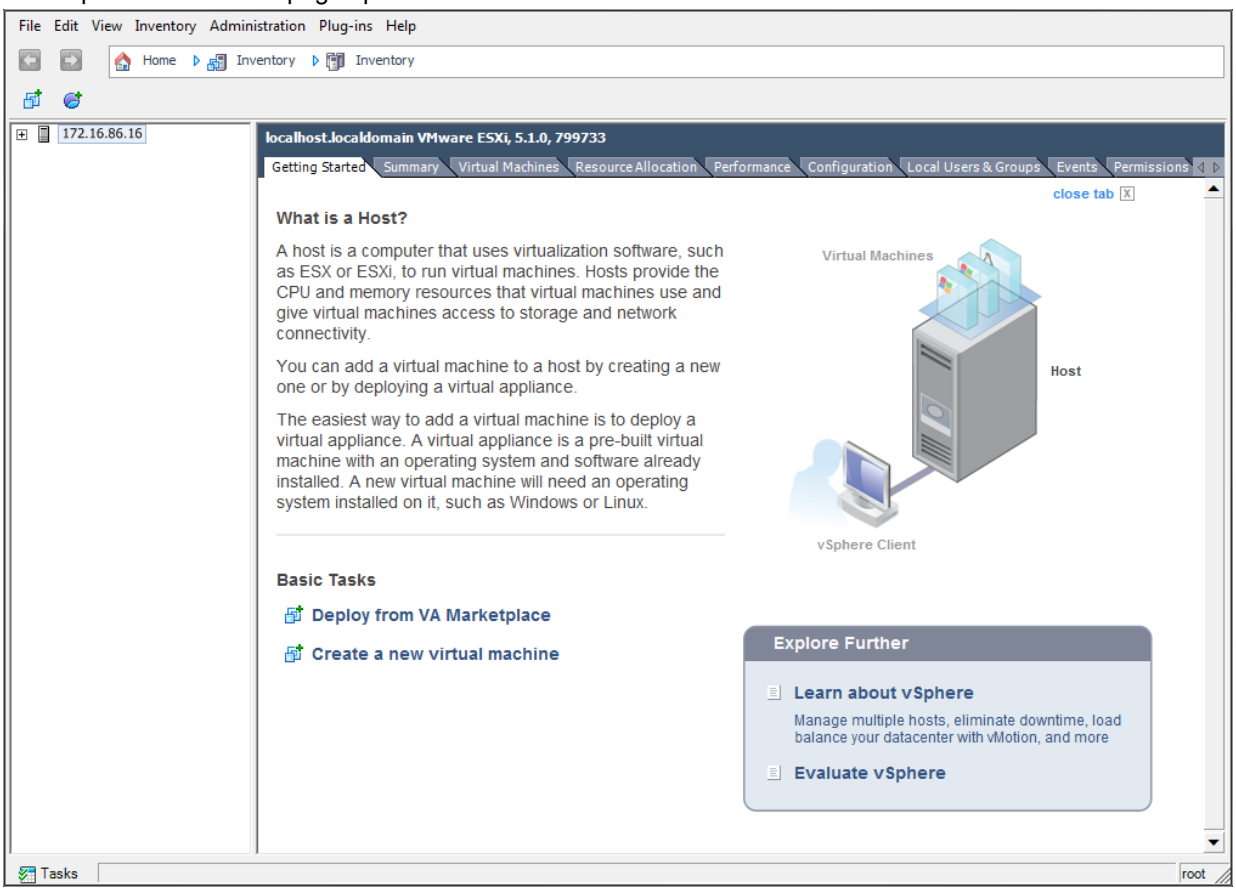
The following topics are included in this section:

Open the FortiGate VM OVF file with the vSphere client

To deploy the FortiGate VM OVF template:

1. Launch the VMware vSphere client, enter the IP address or host name of your server, enter your user name and password and select **Login**.

   The vSphere client home page opens.

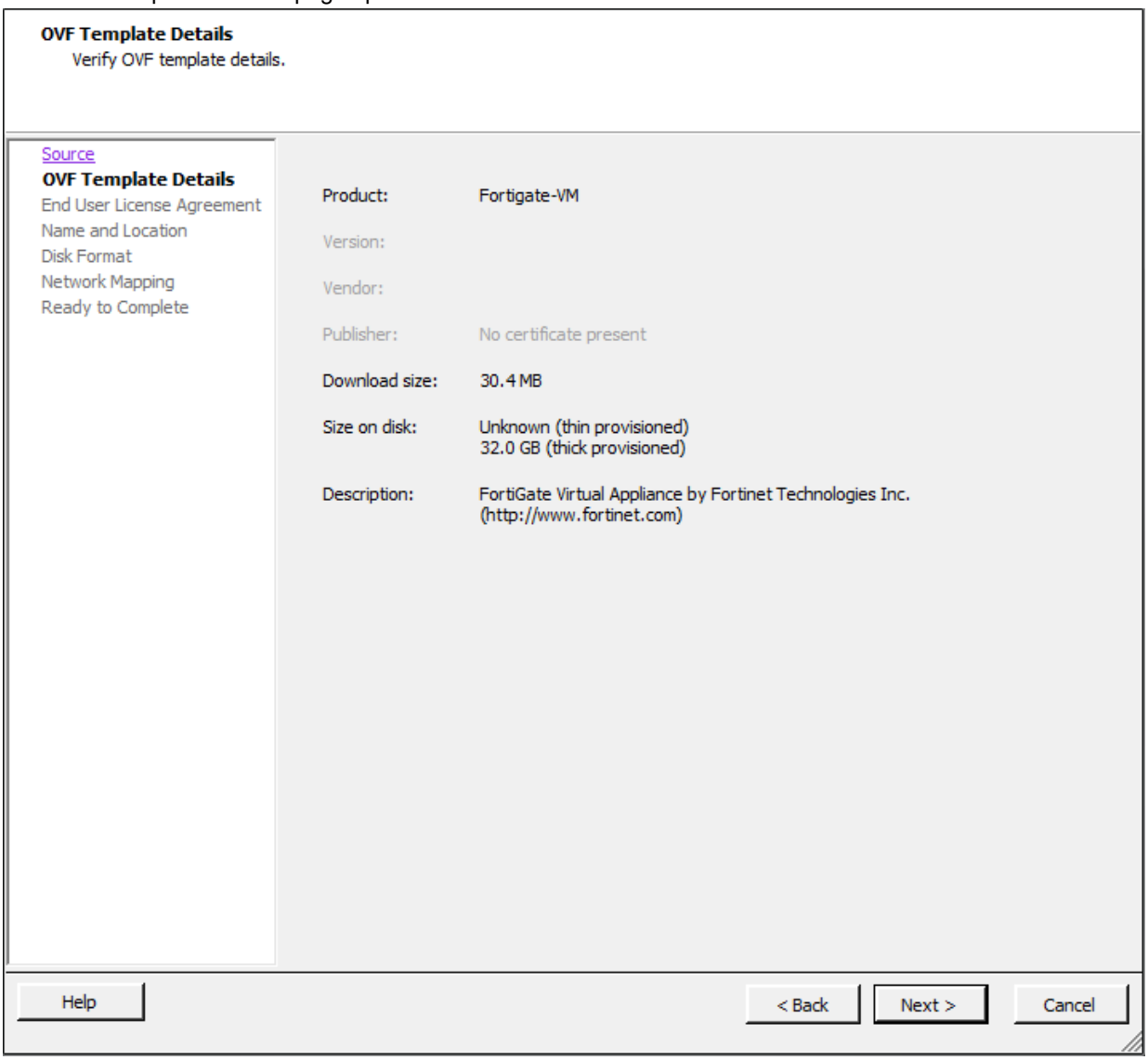


2. Select **File > Deploy OVF Template** to launch the OVF Template wizard.

The OVF Template **Source** page opens.

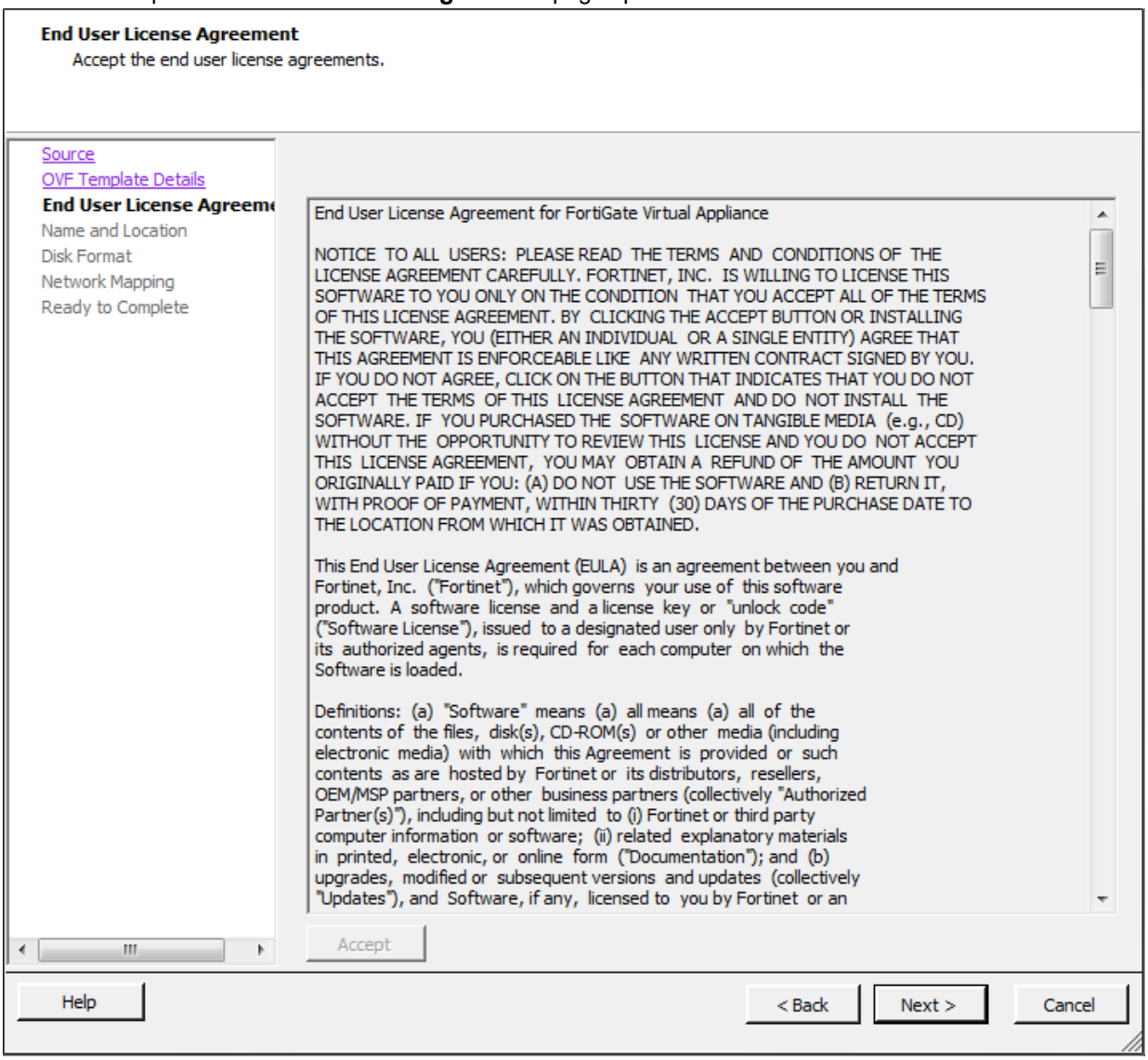
3. Select the source location of the OVF file. Select **Browse** and locate the OVF file on your computer. Select **Next** to continue.

The OVF Template **Details** page opens.



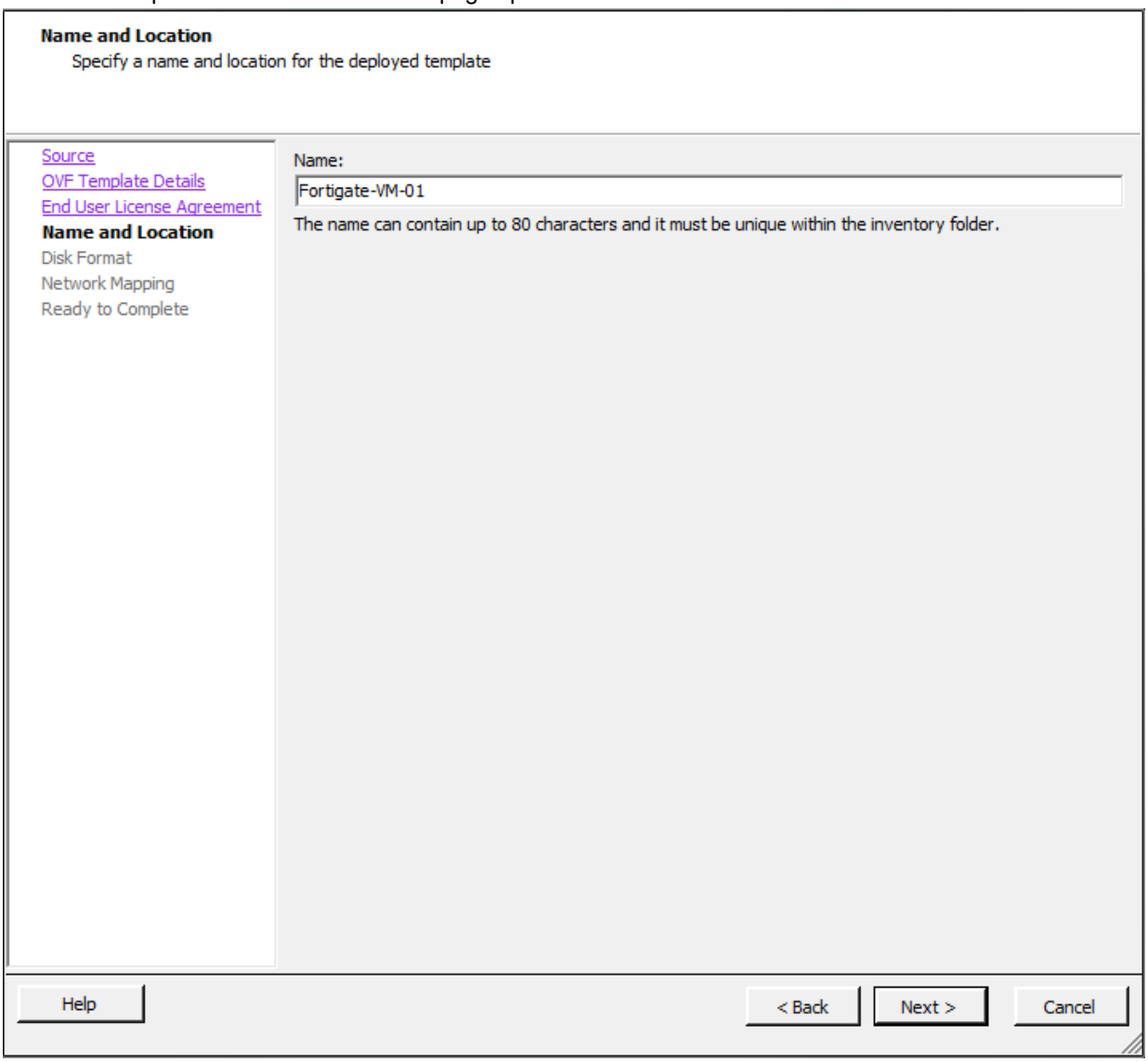
4. Verify the OVF template details. This page details the product name, download size, size on disk, and description. Select **Next** to continue.

The OVF Template **End User License Agreement** page opens.



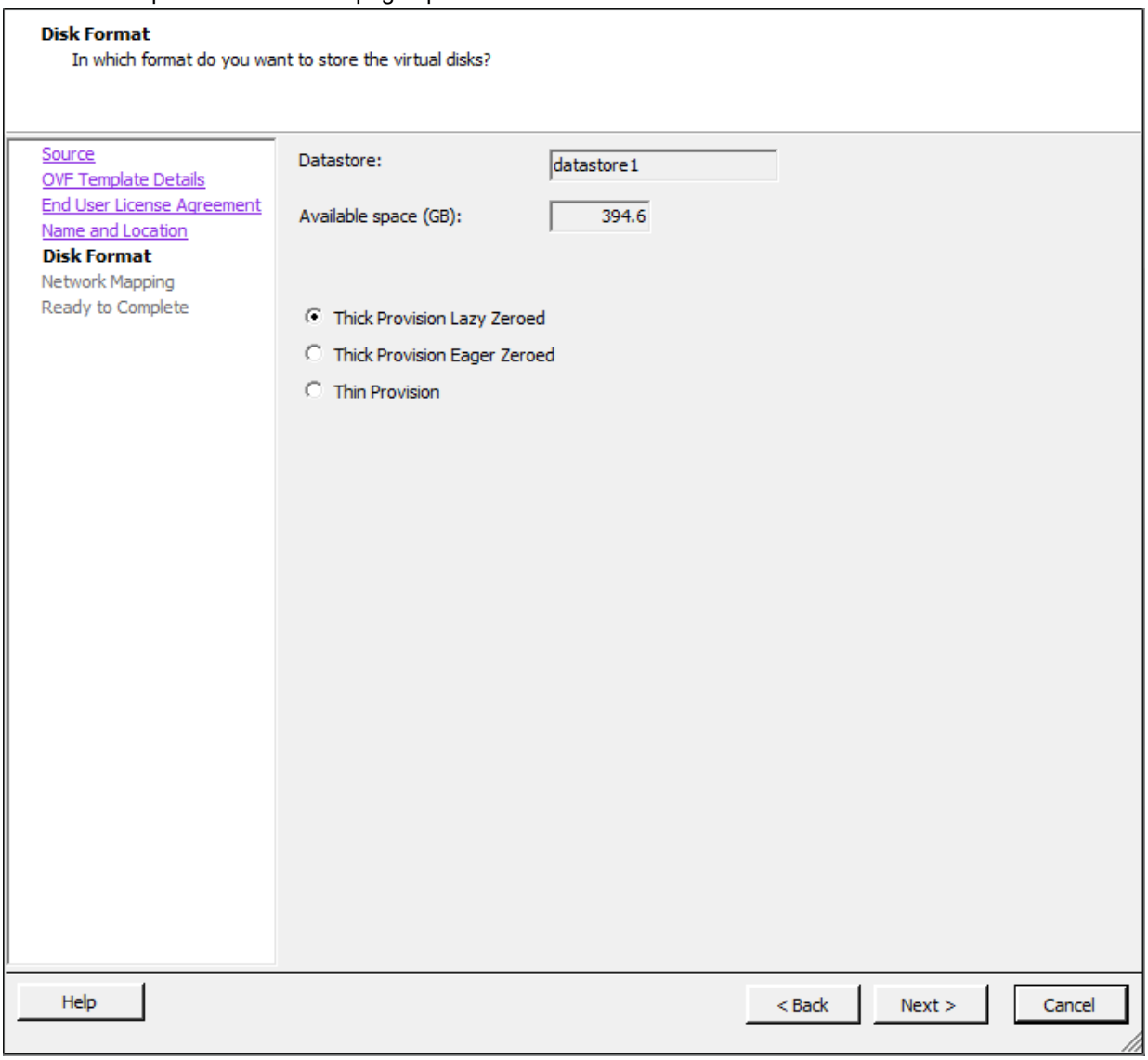
5. Read the end user license agreement for FortiGate VM. Select **Accept** and then select **Next** to continue.

The OVF Template **Name and Location** page opens.



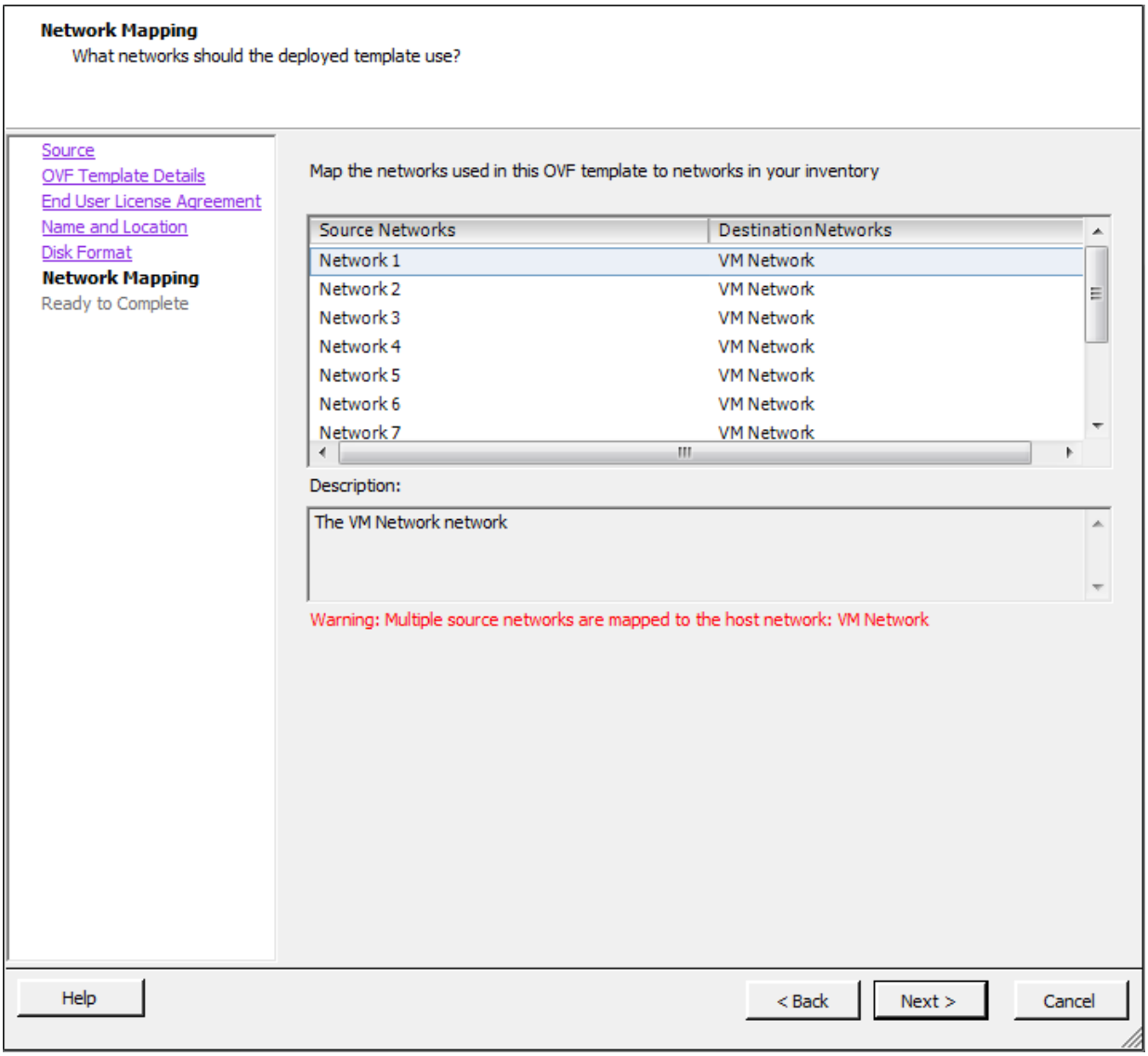
6. Enter a name for this OVF template. The name can contain up to 80 characters and it must be unique within the inventory folder. Select **Next** to continue.

The OVF Template **Disk Format** page opens.



7. Select one of the following:
   - **Thick Provision Lazy Zeroed**: Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format).
   - **Thick Provision Eager Zeroed**: Allocates the disk space statically (no other volumes can take the space), and writes zeros to all the blocks.
   - **Thin Provision**: Allocates the disk space only when a write occurs to a block, but the total volume size is reported by VMFS to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Note that once a Thin Provisioned block is allocated, it remains on the volume regardless if you have deleted data, etc.
8. Select **Next** to continue.

   The OVF Template **Network Mapping** page opens.

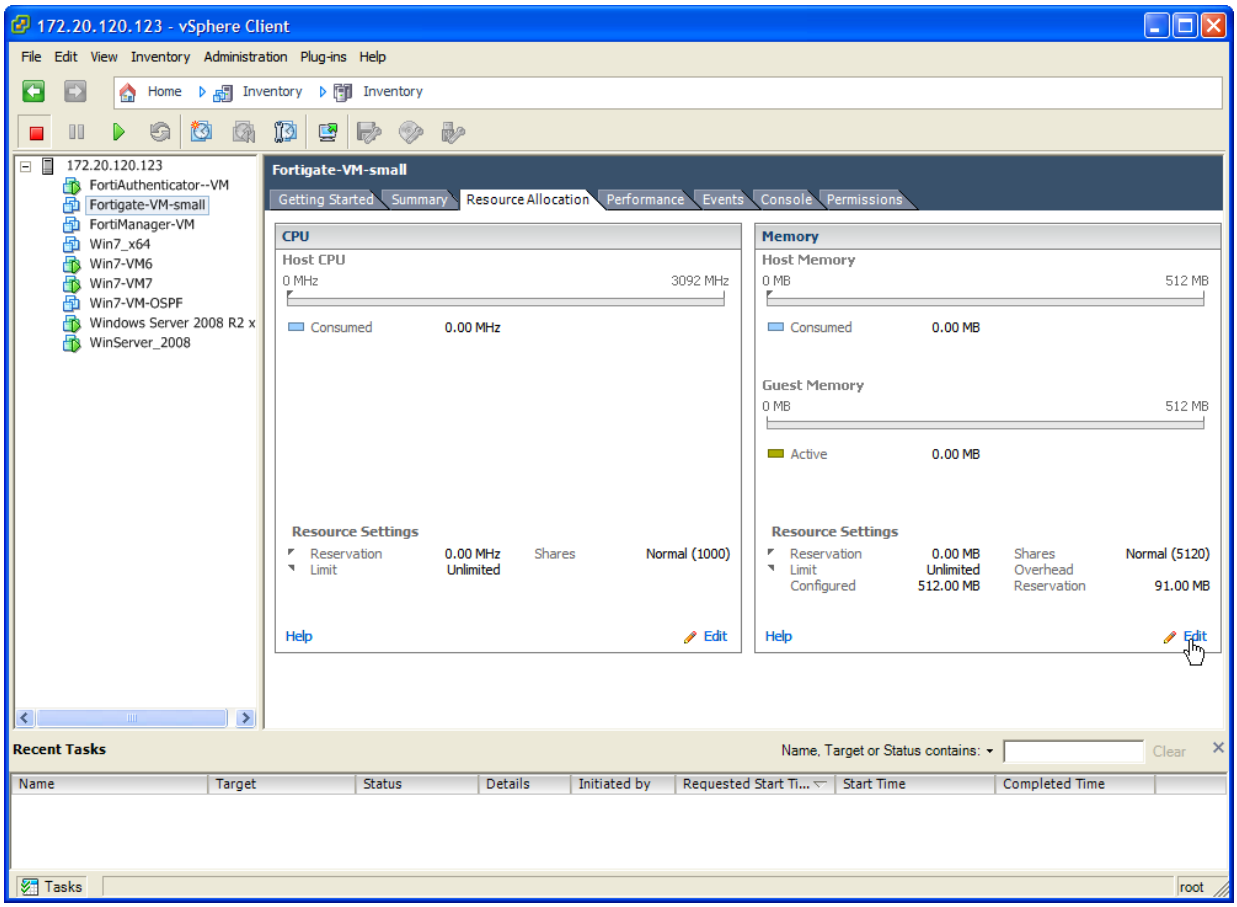


9. Map the networks used in this OVF template to networks in your inventory. Network 1 maps to port1 of the FortiGate VM. You must set the destination network for this entry to access the device console. Select **Next** to continue.

   The OVF Template **Ready to Complete** page opens.
10. Review the template configuration. Make sure that **Power on after deployment** is not enabled. You might need to configure the FortiGate VM hardware settings prior to powering on the FortiGate VM.
11. Select **Finish** to deploy the OVF template. You will receive a **Deployment Completed Successfully** dialog box once the FortiGate VM OVF template wizard has finished.

Configure FortiGate VM hardware settings

Before powering on your FortiGate VM you must configure the virtual memory, virtual CPU, and virtual disk configuration to match your FortiGate VM license.


172.20.120.123 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
172.20.120.123
FortiAuthenticator--VM
Fortigate-VM-small
FortiManager-VM
Win7_x64
Win7-VM6
Win7-VM7
Win7-VM-OSPF
Windows Server 2008 R2 x
WinServer_2008
Fortigate-VM-small
Getting Started Summary Resource Allocation Performance Events Console Permissions
CPU
Host CPU
0 MHz 3092 MHz
Consumed 0.00 MHz
Resource Settings
Reservation 0.00 MHz Shares Normal (1000)
Limit Unlimited
Help Edit
Memory
Host Memory
0 MB 512 MB
Consumed 0.00 MB
Guest Memory
0 MB 512 MB
Active 0.00 MB
Resource Settings
Reservation 0.00 MB Shares Normal (5120)
Limit Unlimited Overhead
Configured 512.00 MB Reservation 91.00 MB
Help Edit
Recent Tasks
Name, Target or Status contains: Clear
Name Target Status Details Initiated by Requested Start Ti... Start Time Completed Time
Tasks
root

Transparent mode VMware configuration

If you want to use your FortiGate-VM in transparent mode, your VMware server's virtual switches must operate in promiscuous mode. This permits these interfaces to receive traffic that will pass through the FortiGate unit but was not addressed to the FortiGate unit.

In VMware, promiscuous mode must be explicitly enabled:

1. In the vSphere client, select your VMware server in the left pane and then select the **Configuration** tab in the right pane.
2. In **Hardware**, select **Networking**.
3. Select **Properties** of vSwitch0.
4. In the **Properties** window left pane, select **vSwitch** and then select **Edit**.
5. Select the **Security** tab, set **Promiscuous Mode** to **Accept**, then select **OK**.
6. Select **Close**.
7. Repeat steps 3 through 6 for other vSwitches that your transparent mode FortiGate-VM uses.

High Availability VMware configuration

If you want to combine two or more FortiGate-VM instances into a FortiGate Clustering Protocol (FGCP) High Availability (HA) cluster the VMware server's virtual switches used to connect the heartbeat interfaces must operate in promiscuous mode. This permits HA heartbeat communication between the heartbeat interfaces. HA heartbeat packets are non-TCP packets that use Ethertype values 0x8890, 0x8891, and 0x8890. The FGCP uses link-local IPv4 addresses in the 169.254.0.x range for HA heartbeat interface IP addresses.

To enable promiscuous mode in VMware:

1. In the vSphere client, select your VMware server in the left pane and then select the **Configuration** tab in the right pane.
2. In **Hardware**, select **Networking**.
3. Select **Properties** of a virtual switch used to connect heartbeat interfaces.
4. In the **Properties** window left pane, select **vSwitch** and then select **Edit**.
5. Select the **Security** tab, set **Promiscuous Mode** to **Accept**, then select **OK**.
6. Select **Close**.

You must also set the virtual switches connected to other FortiGate interfaces to allow MAC address changes and to accept forged transmits. This is required because the FGCP sets virtual MAC addresses for all FortiGate interfaces and the same interfaces on the different VM instances in the cluster will have the same virtual MAC addresses.

To make the required changes in VMware:

1. In the vSphere client, select your VMware server in the left pane and then select the **Configuration** tab in the right pane.
2. In **Hardware**, select **Networking**.
3. Select **Properties** of a virtual switch used to connect FortiGate VM interfaces.
4. Set **MAC Address Changes**to**Accept**.
5. Set **Forged Transmits** to **Accept**.

Power on your FortiGate VM

You can now proceed to power on your FortiGate VM. There are several ways to do this:

- Select the name of the FortiGate VM you deployed in the inventory list and select **Power on the virtual machine** in the **Getting Started** tab.
- In the inventory list, right-click the name of the FortiGate VM you deployed, and select **Power > Power On**.
- Select the name of the FortiGate VM you deployed in the inventory list. Click the **Power On** button on the toolbar.

Select the Console tab to view the console. To enter text, you must click in the console pane. The mouse is then captured and cannot leave the console screen. As the FortiGate console is text-only, no mouse pointer is visible. To release the mouse, press Ctrl-Alt.

Deployment example – MS Hyper-V

Once you have downloaded the FGT_VMxx_HV-v5-build0xxx-FORTINET.out.hyperv.zip file and extracted the package contents to a folder on your Microsoft server, you can deploy the VHD package to your Microsoft Hyper-V environment.

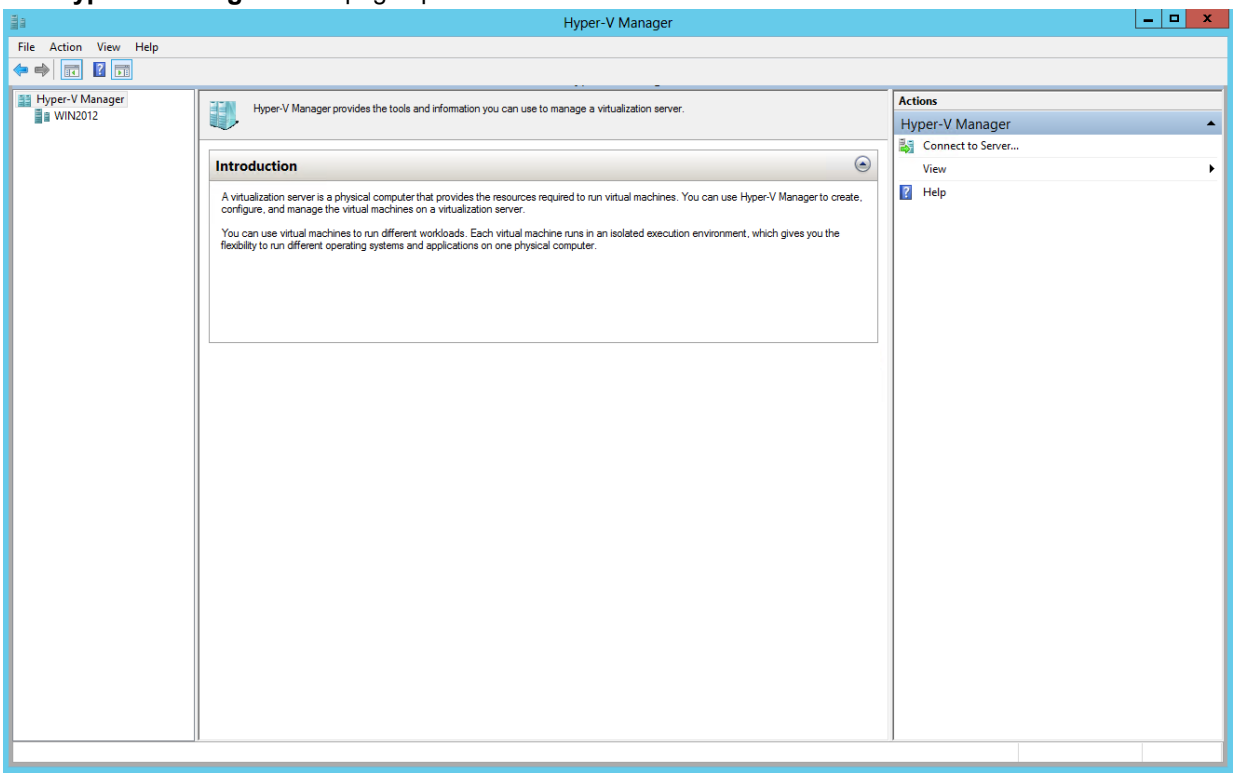
The following topics are included in this section:

Create the FortiGate VM virtual machine

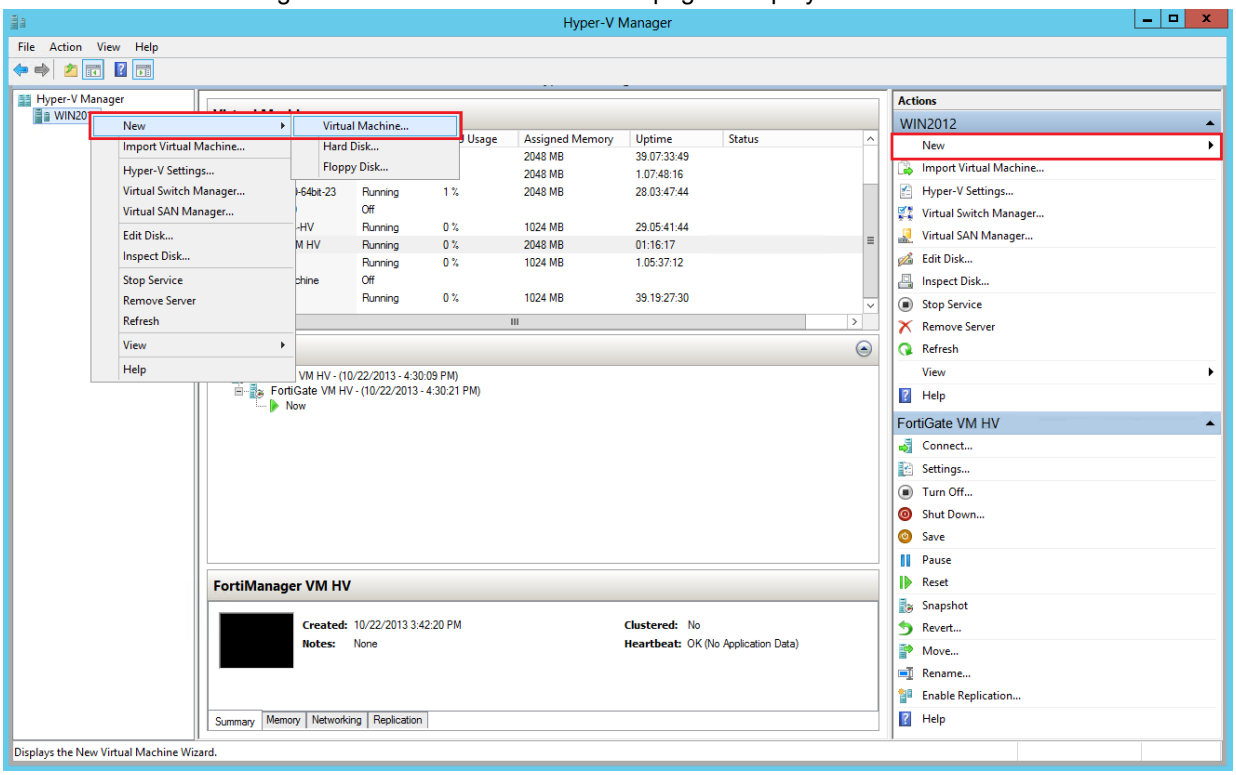
To create the FortiGate VM virtual machine:

1. Launch the Hyper-V Manager in your Microsoft server.

   The **Hyper-V Manager** home page opens.

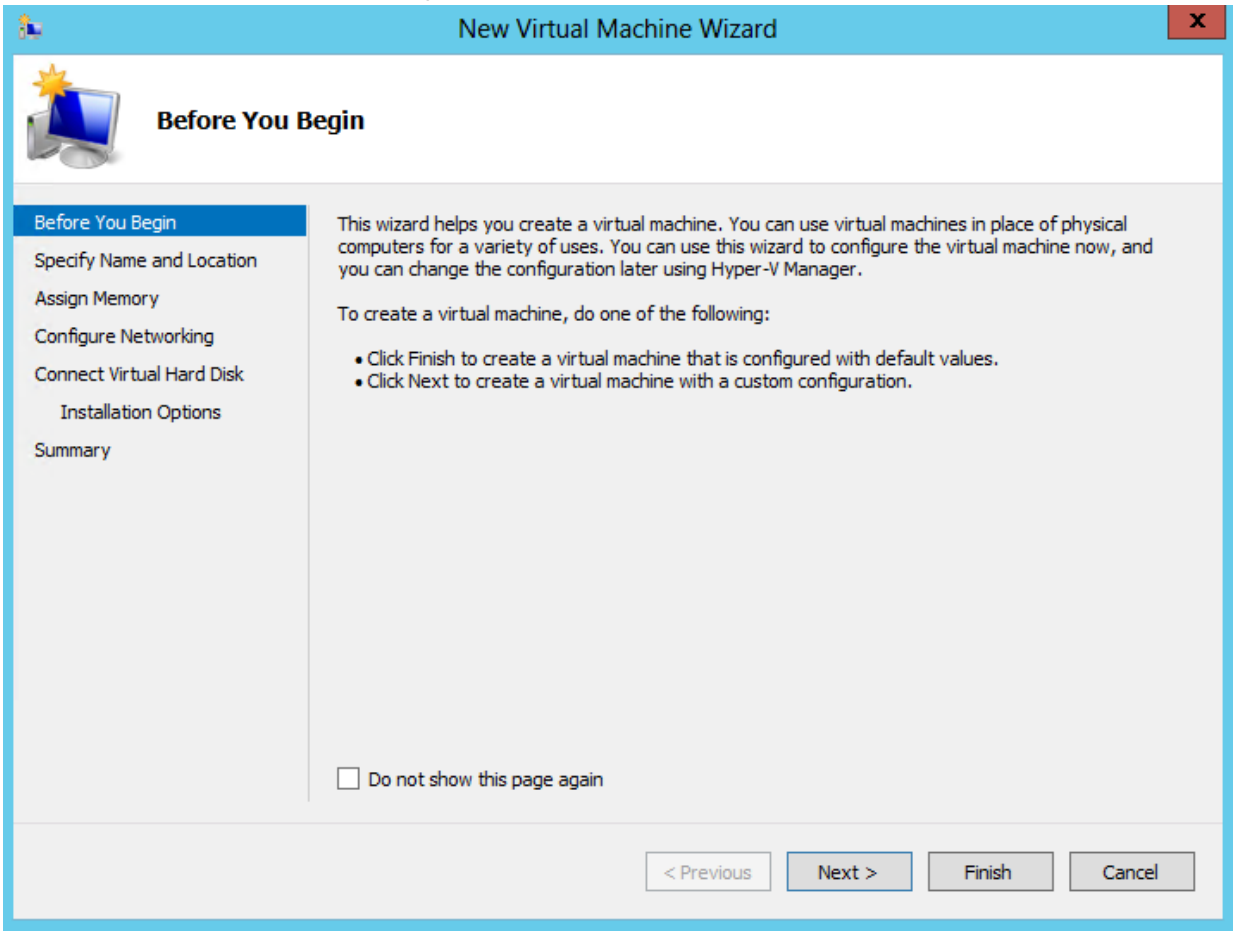


2. Select the server in the right-tree menu. The server details page is displayed.



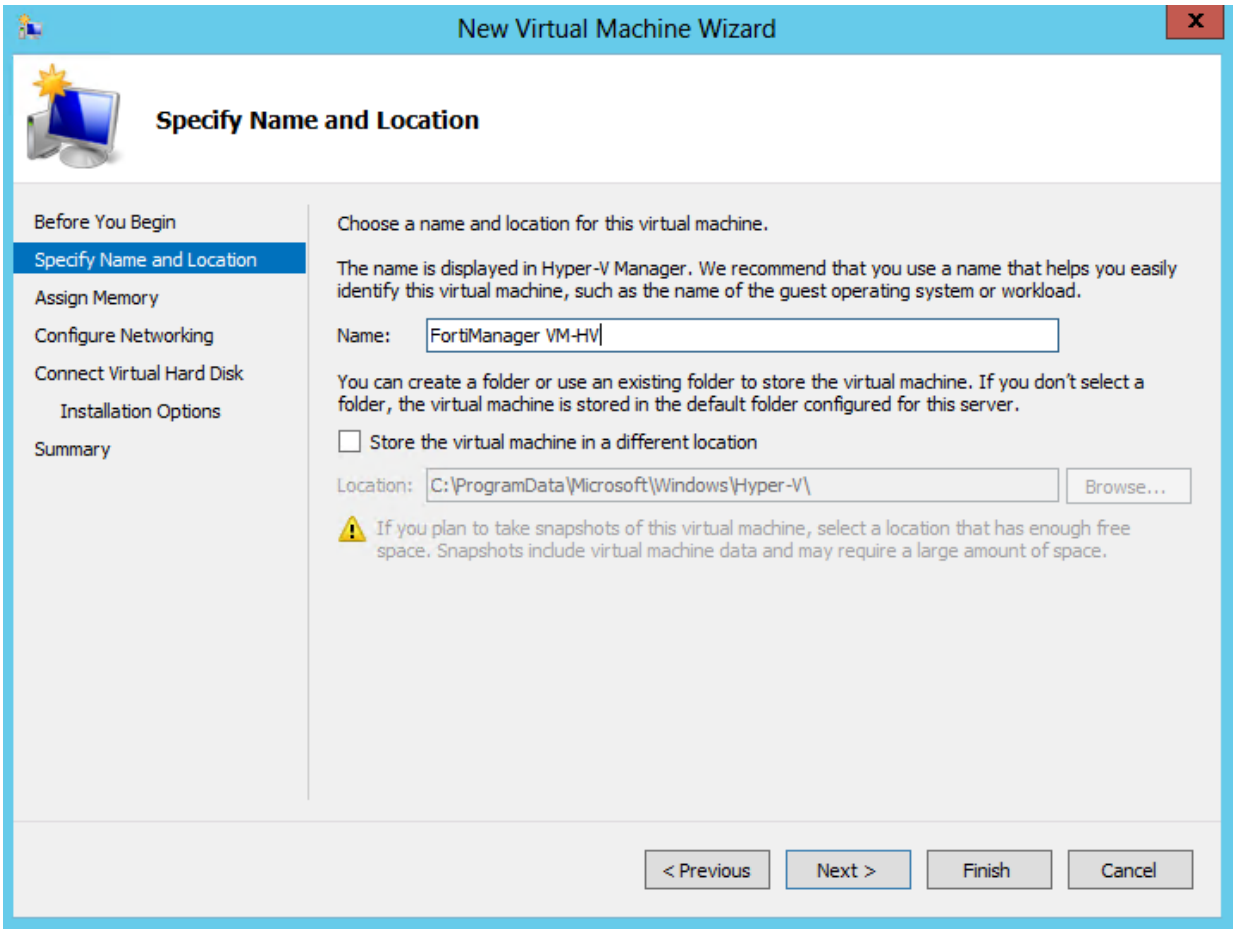
3. Right-click the server and select **New and select Virtual Machine** from the menu. Optionally, in the **Actions** menu, select **New** and select **Virtual Machine** from the menu.

The **New Virtual Machine Wizard** opens.



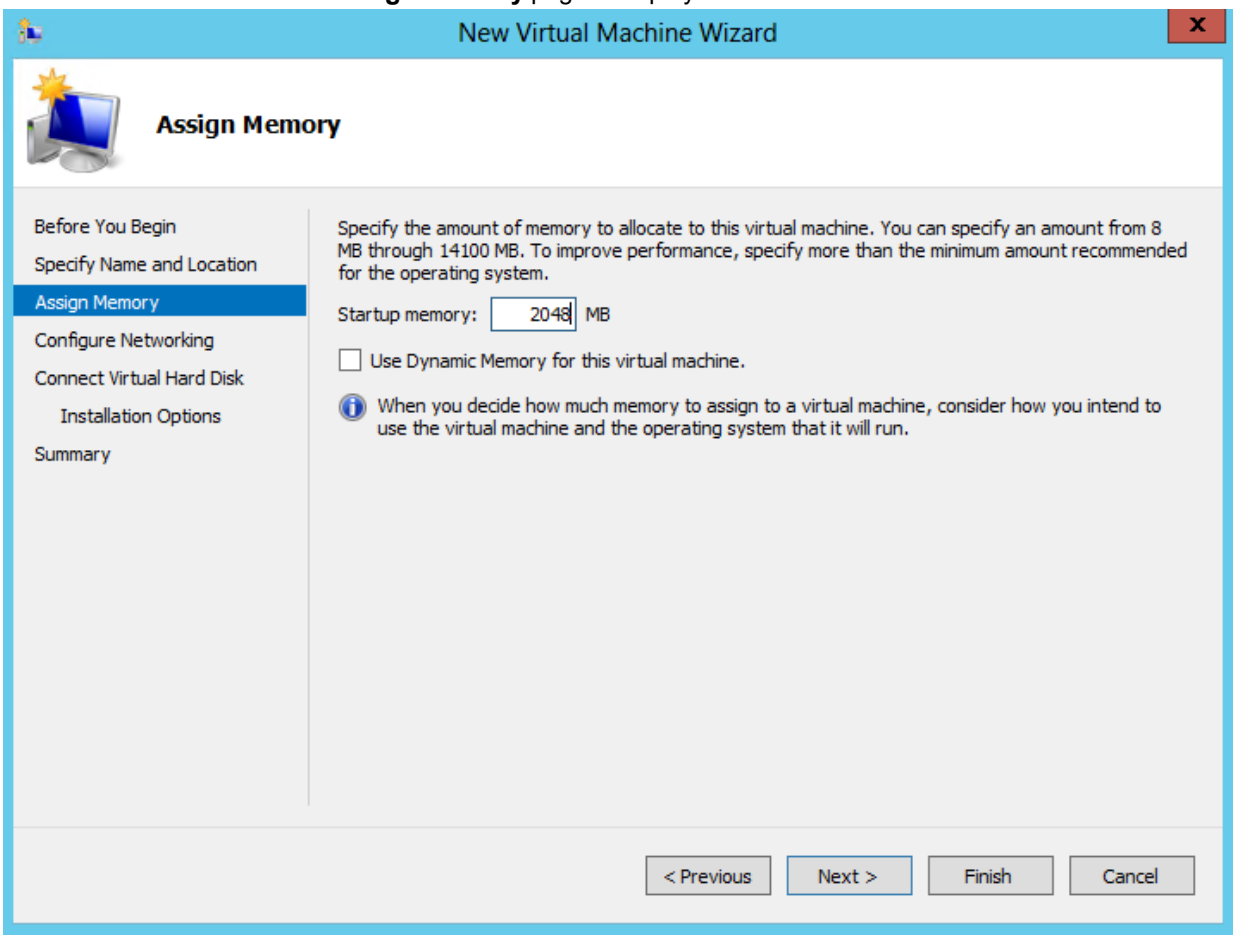
4. Select **Next** to create a virtual machine with a custom configuration.

   The **Specify Name and Location** page is displayed.



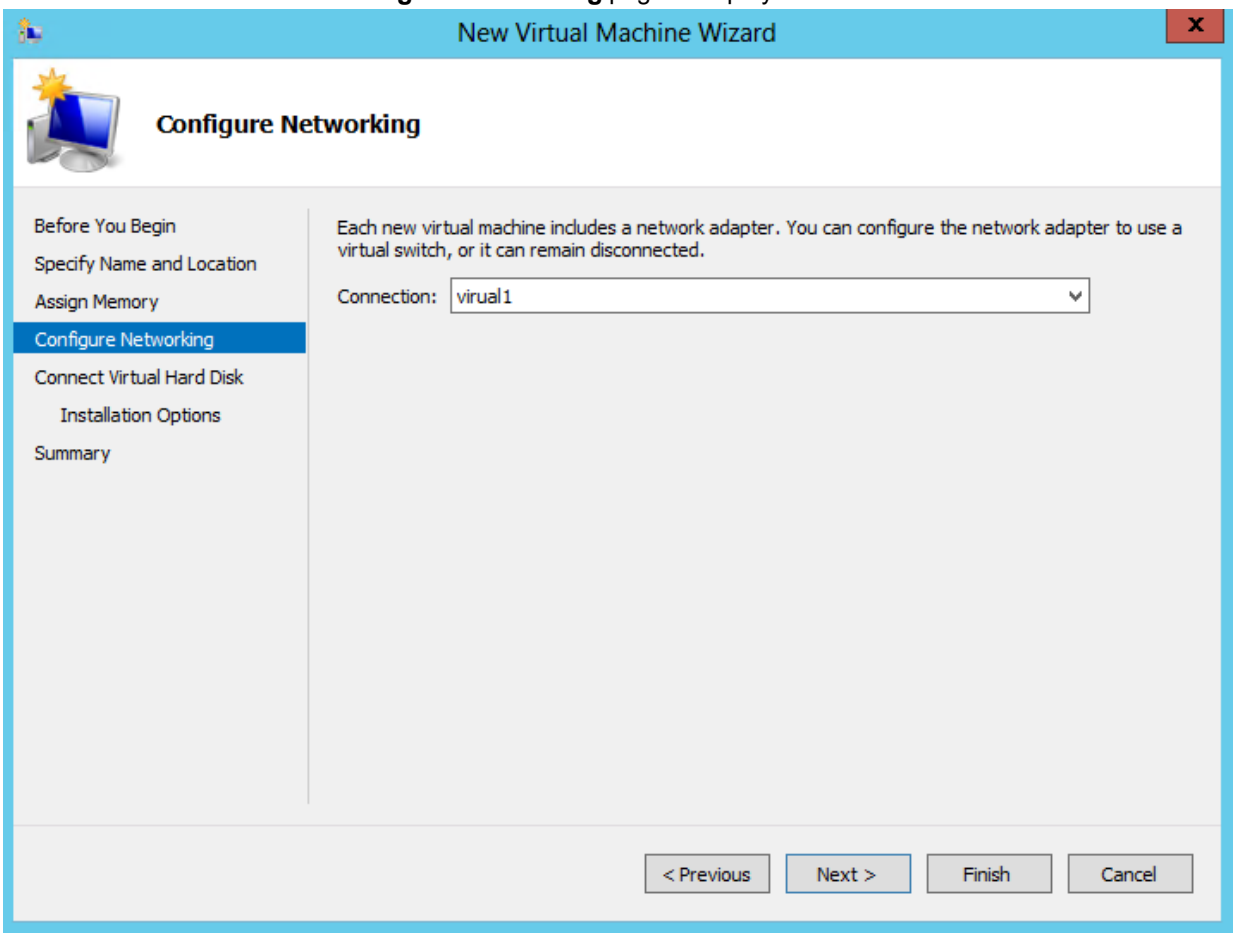
5. Enter a name for this virtual machine. The name is displayed in the Hyper-V Manager.

Select **Next** to continue. The **Assign Memory** page is displayed.



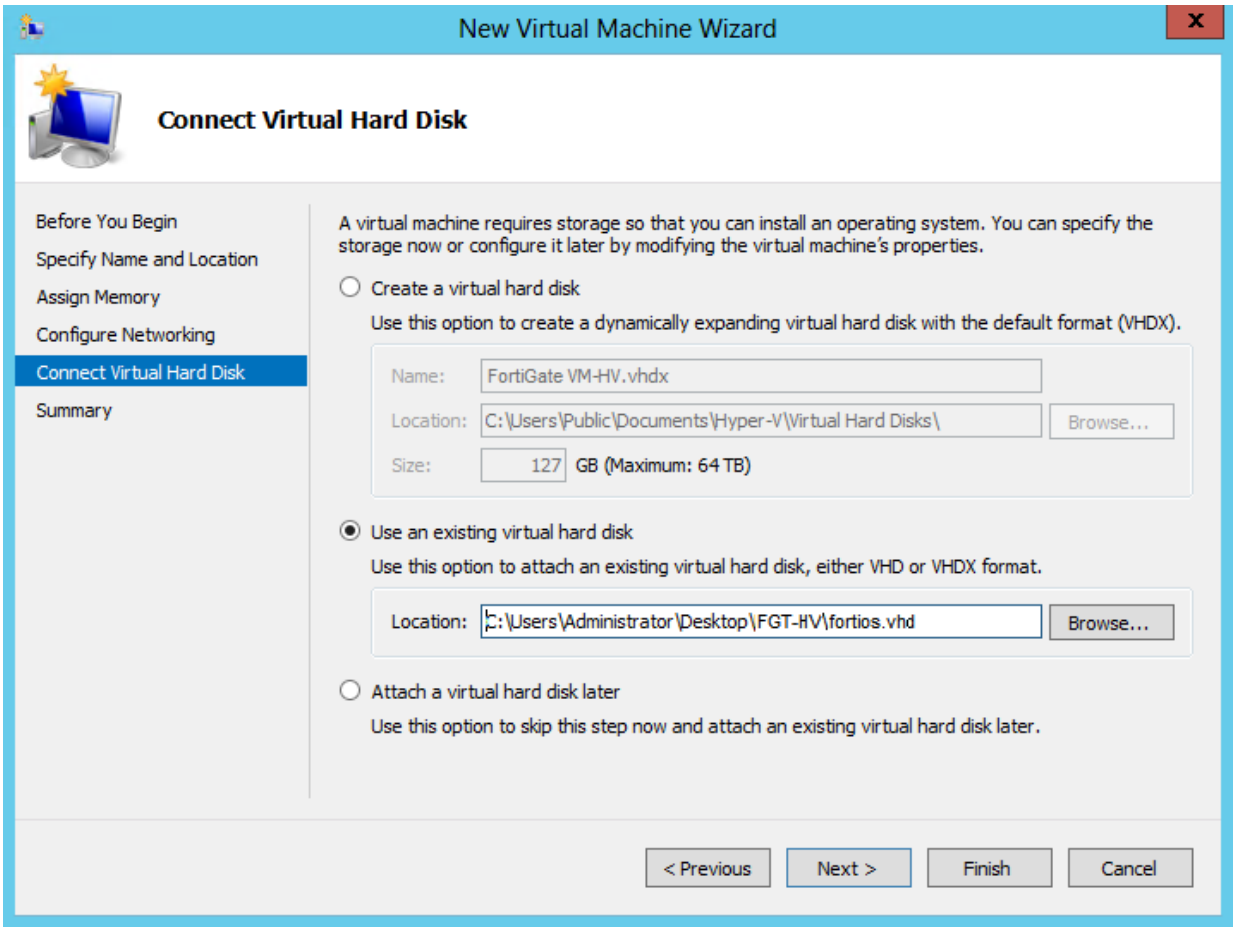
6. Specify the amount of memory to allocate to this virtual machine. The default memory for FortiGate VM is 1GB (1024MB).

Select **Next** to continue. The **Configure Networking** page is displayed.



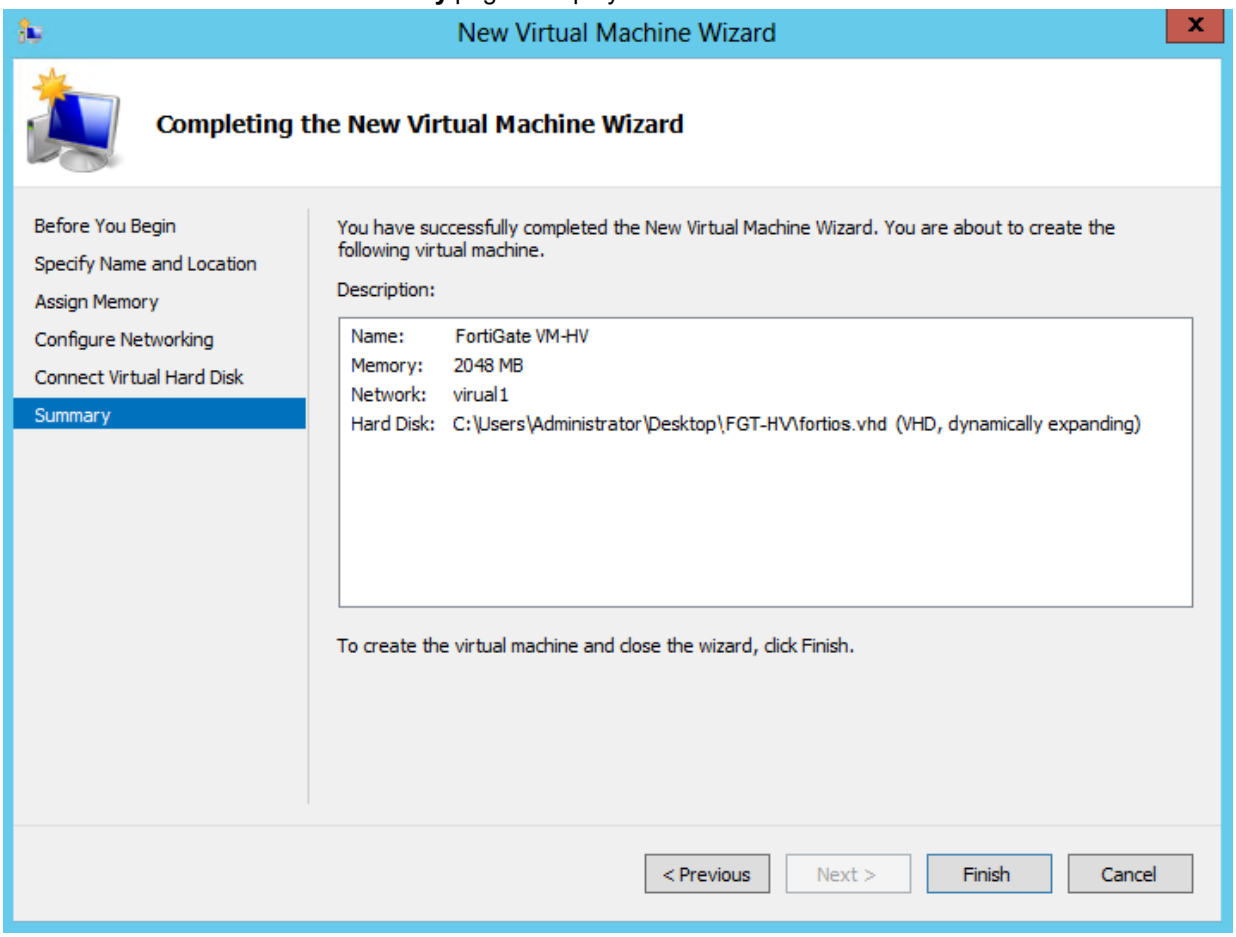
7. Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected. FortiGate VM requires four network adapters. You must configure network adapters in the **Settings** page.

   Select **Next** to continue. The **Connect Virtual Hard Disk** page is displayed.



8. Select to use an existing virtual hard disk and browse for the `fortios.vhd` file that you downloaded from the Fortinet Customer Service & Support portal.

Select **Next** to continue. The **Summary** page is displayed.



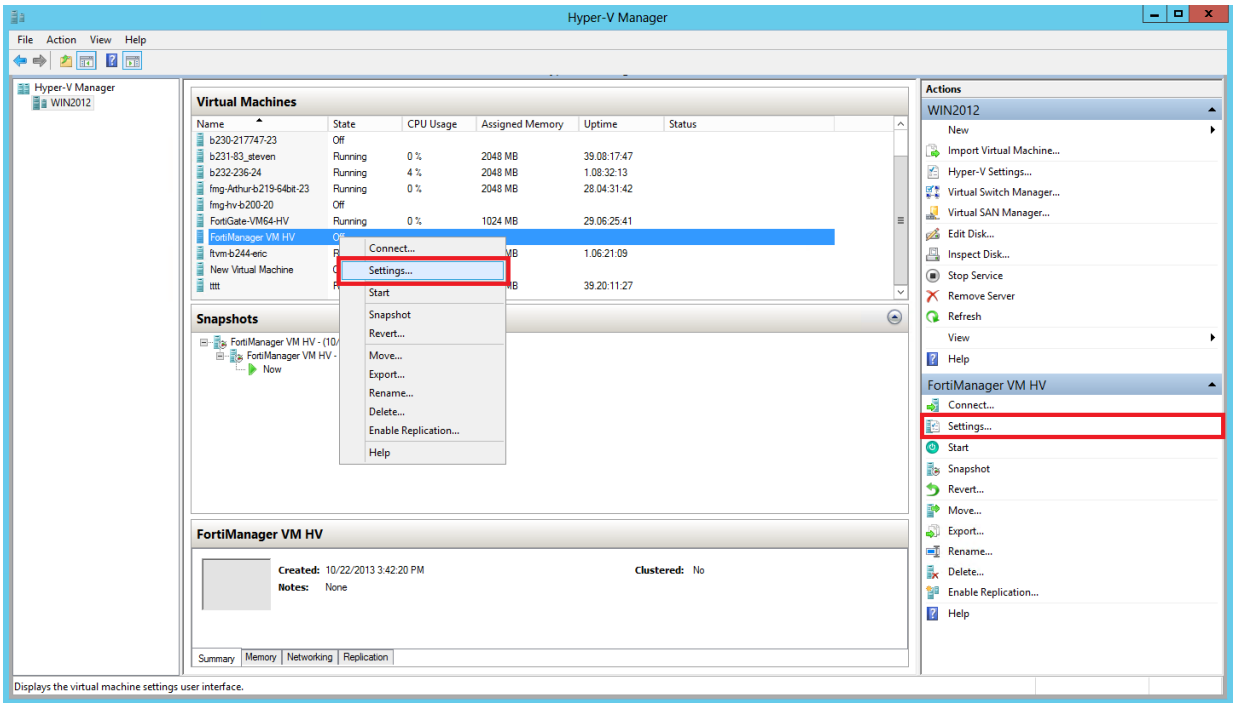
9. To create the virtual machine and close the wizard, select **Finish**.

Configure FortiGate VM hardware settings

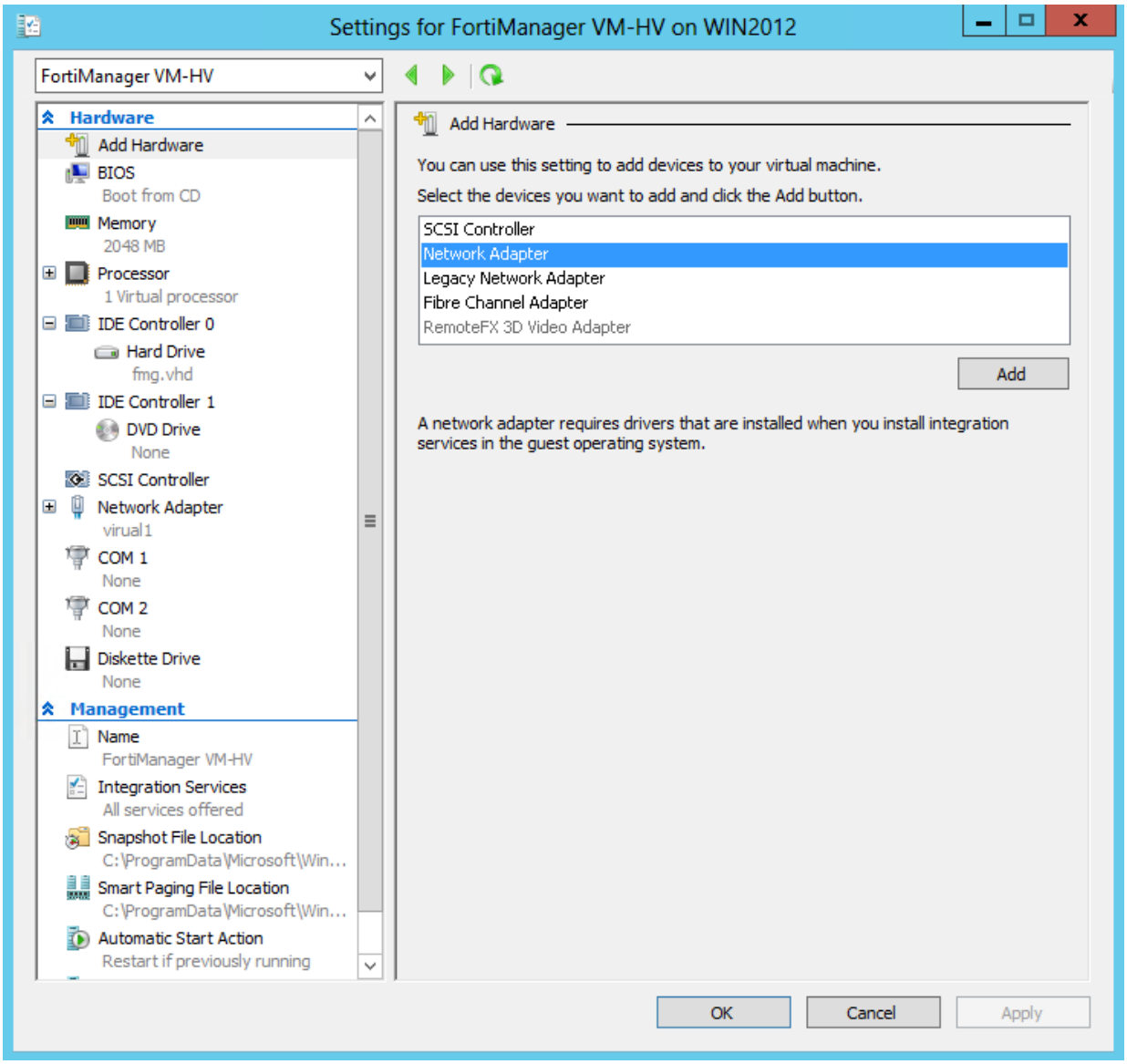
Before powering on your FortiGate VM you must configure the virtual memory, virtual CPU, and virtual disk configuration to match your FortiGate VM license.

To configure settings for FortiGate VM on the server:

1. In the Hyper-V Manager, locate the name of the virtual machine, right-click the entry, and select **Settings** from the menu. Optionally, you can select the virtual machine and select **Settings** in the **Actions** menu.



The **Settings** page is displayed.



2. Configure virtual processors, network adapters, and virtual hard drive settings.
3. Select **Apply** to save the settings and then select **OK** to close the settings page.

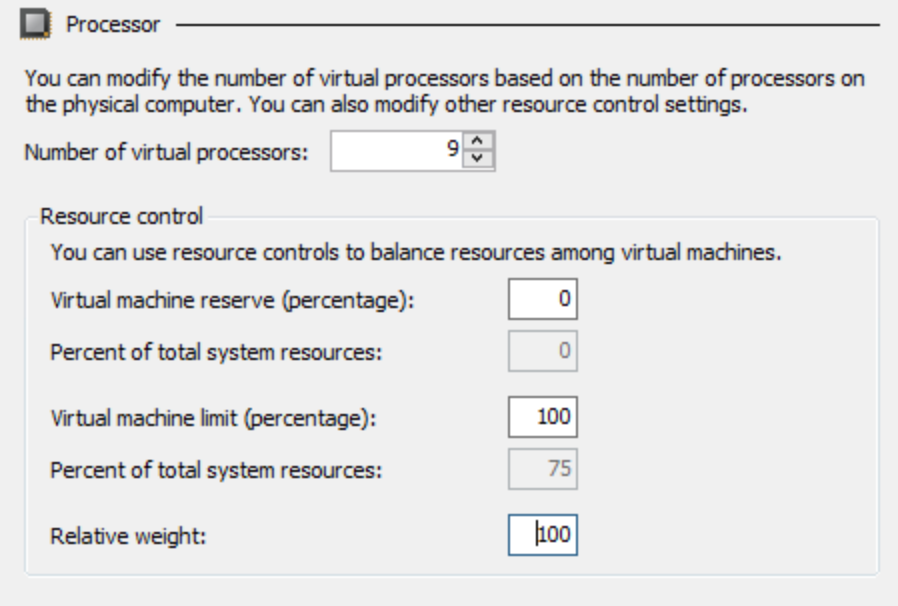
FortiGate VM virtual processors

You must configure FortiGate VM virtual processors in the server settings page. The number of processors is dependent on your server environment.

Configure FortiGate VM virtual processors:

1. In the **Settings** page, select **Processor** from the **Hardware** menu.

   The **Processor** page is displayed.



2. Configure the number of virtual processors for the FortiGate VM virtual machine. Optionally, you can use resource controls to balance resources among virtual machines.
3. Select **Apply** to save the settings.

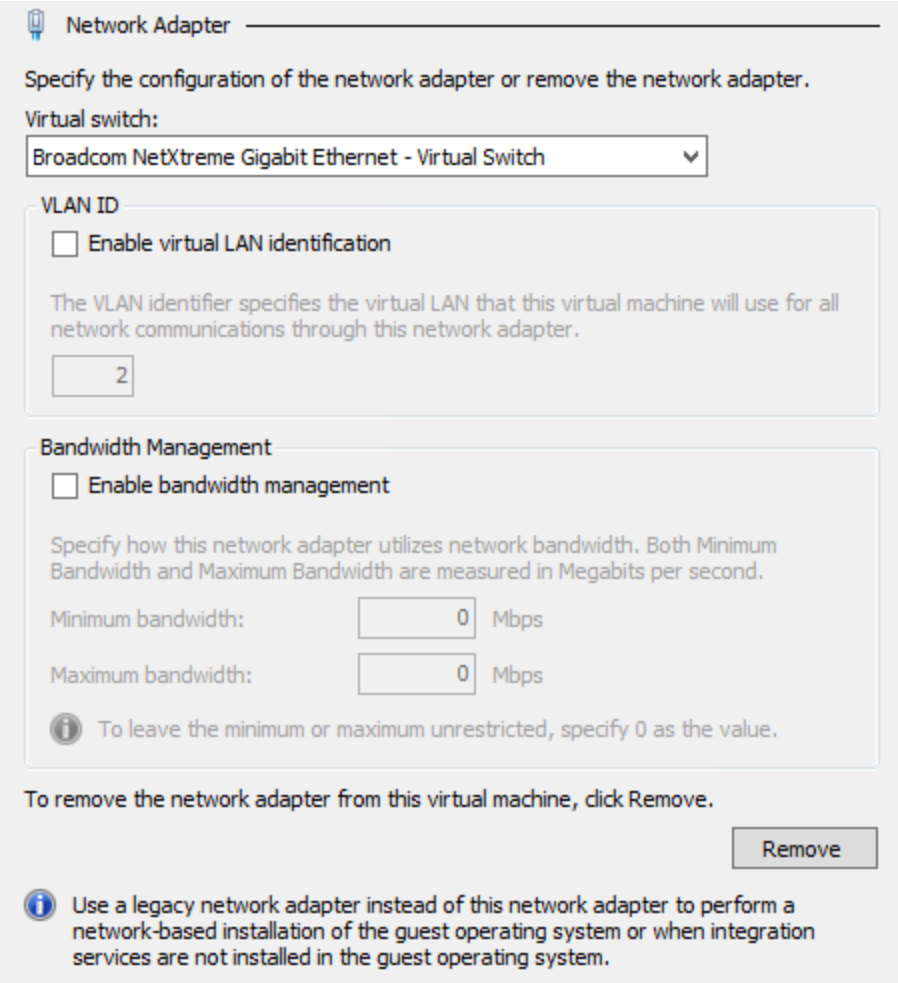
FortiGate VM network adapters

You must configure FortiGate VM network adapters in the server settings page. FortiGate VM supports four network adapters.

Configure FortiGate VM network adapters:

1. In the **Settings** page, select **Add Hardware** from the **Hardware** menu, select **Network Adapter** in the device list, and select the **Add** button.

The **Network Adapter** page is displayed.



1. You must manually configure four network adapters for FortiGate VM in the settings page. For each network adapter, select the virtual switch from the drop-down list.
2. Select **Apply** to save the settings.

FortiGate VM virtual hard disk

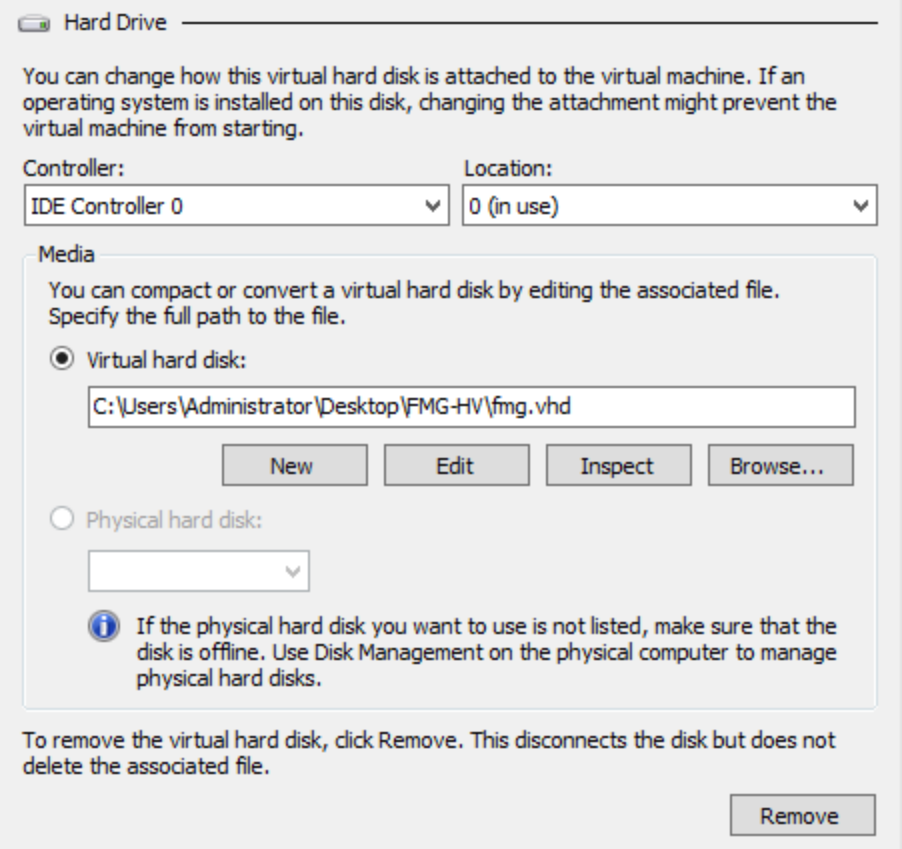
You must configure the FortiGate VM virtual hard disk in the server settings page.

If you know your environment will expand in the future, it is recommended to increase the hard disk size beyond 30GB. The VM license limit is 2TB.

Configure a FortiGate VM virtual hard drive:

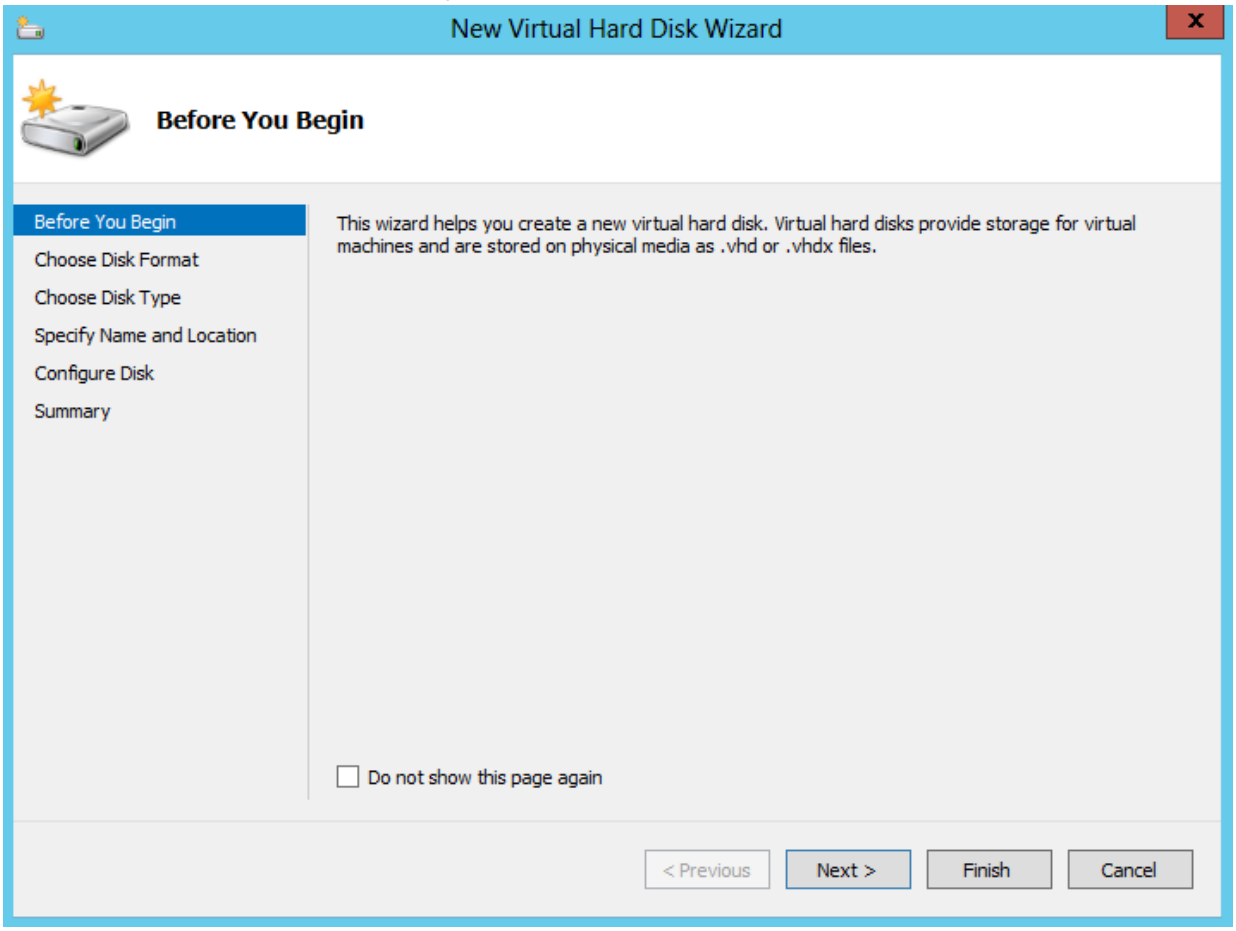
1. In the **Settings** page, select **IDE Controller 0 > Hard Drive** from the **Hardware** menu.

   The **Hard Drive** page is displayed.



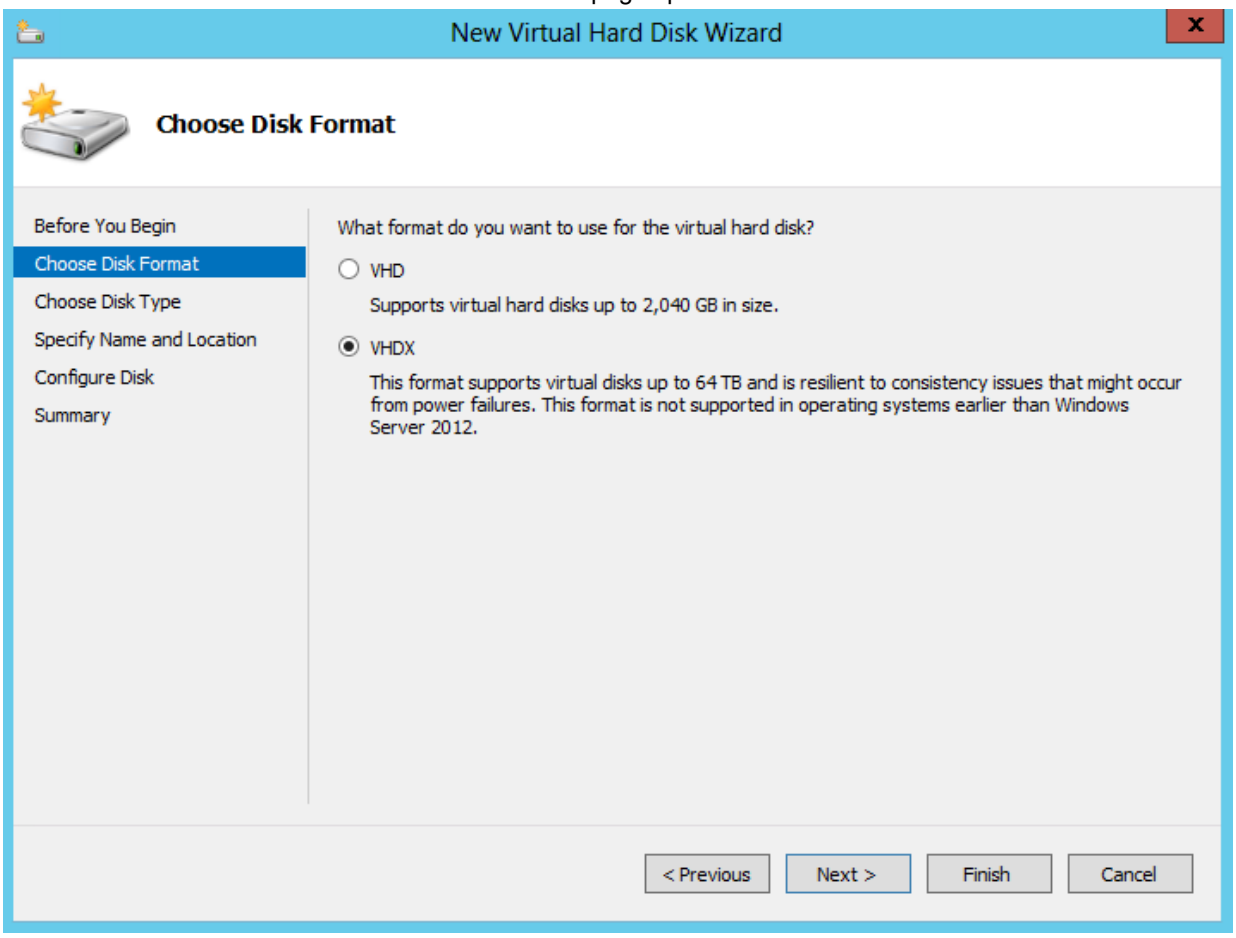
2. Select **New** to create a new virtual hard disk.

The **New Virtual Hard Disk Wizard** opens.



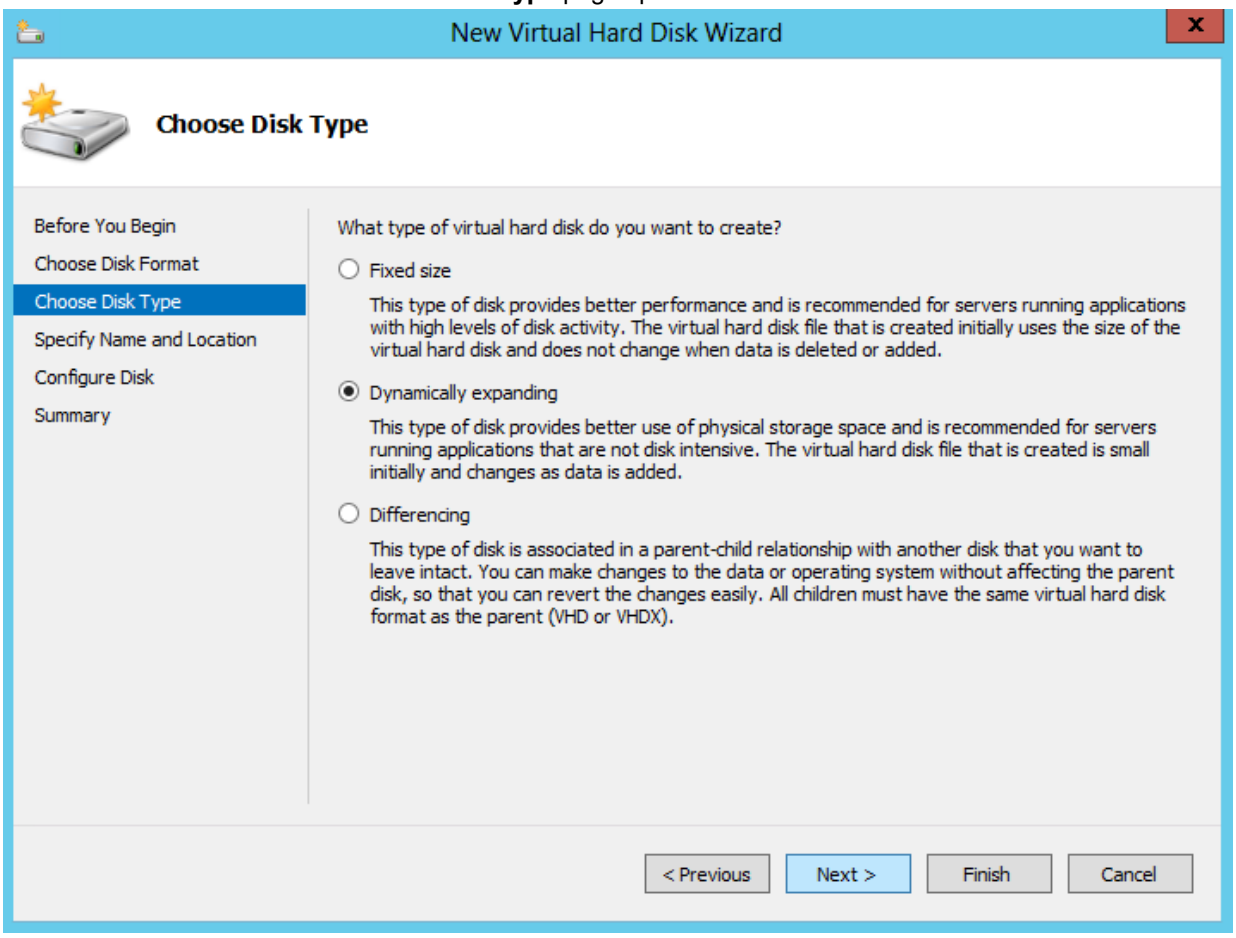
3. This wizard helps you to create a new virtual hard disk.

Select **Next** to continue. The **Choose Disk Format** page opens.



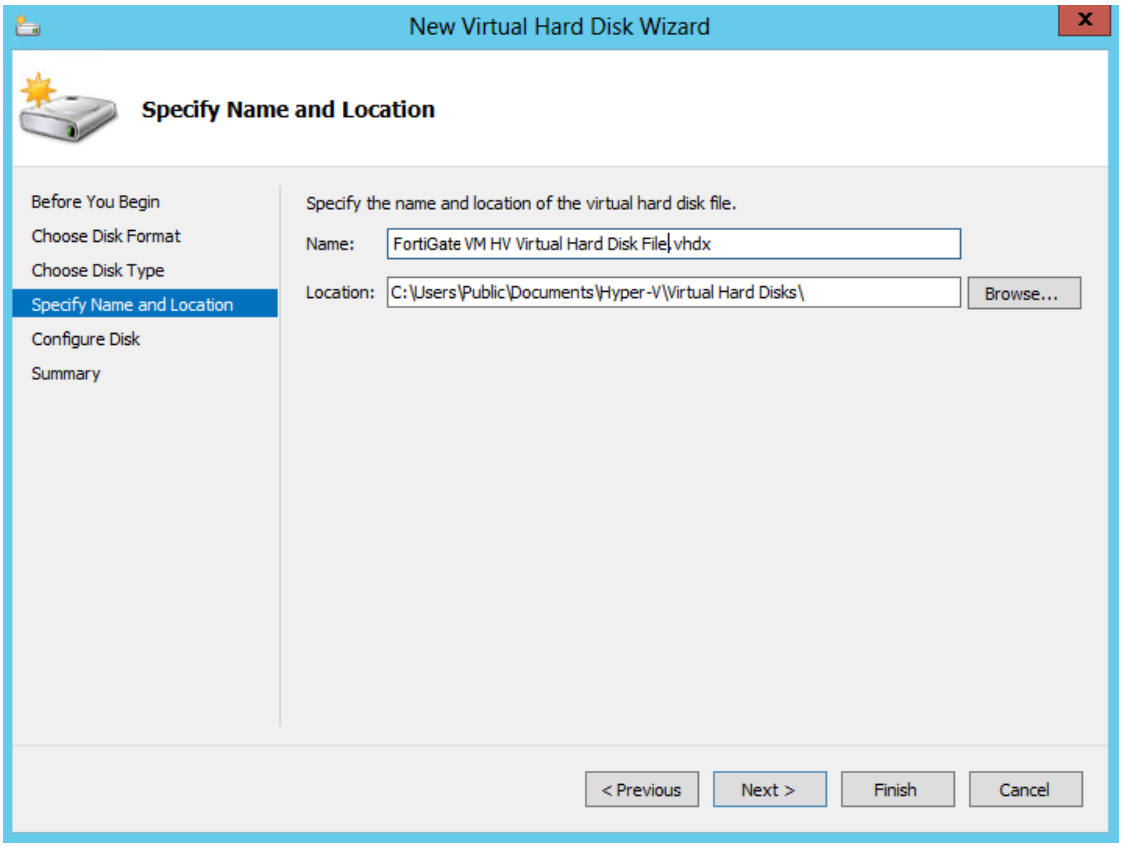
4. Select to use VHDX format virtual hard disks. This format supports virtual disks up to 64TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier than Windows Server 2012. Note that FortiGate-VM does not support hard disks larger than 2TB.

Select **Next** to continue. The **Choose Disk Type** page opens.



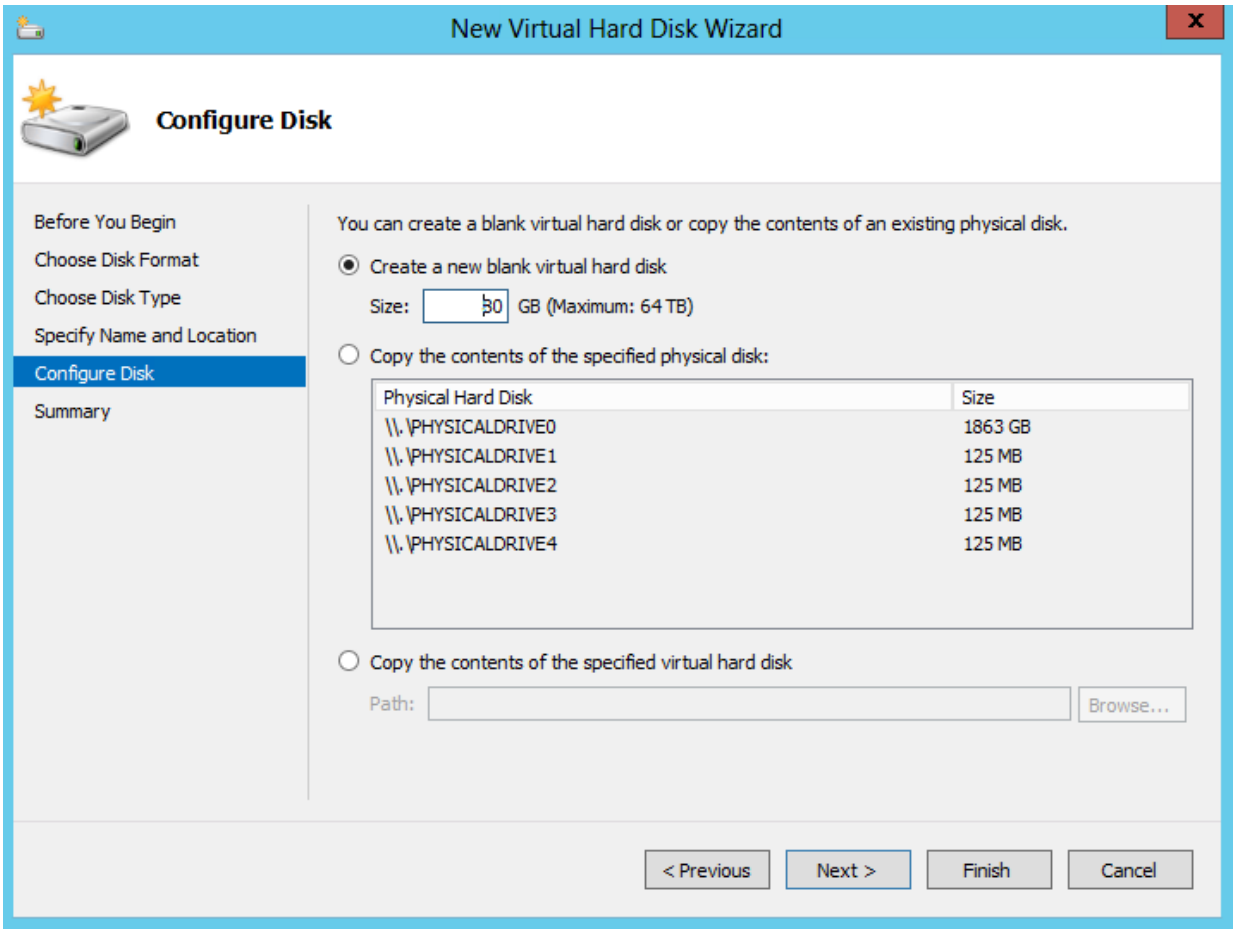
5. Select the type of virtual disk you want to use. Select one of the following disk types:
   - Fixed size: This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.
   - Dynamic expanding: This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual disk file that is created is small initially and changes as data is added.
   - Differencing: This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that you can revert the changes easily. All children must have the same virtual hard disk format as the parent (VHD or VHDX).

   Select **Next** to continue. The **Specify Name and Location** page opens.



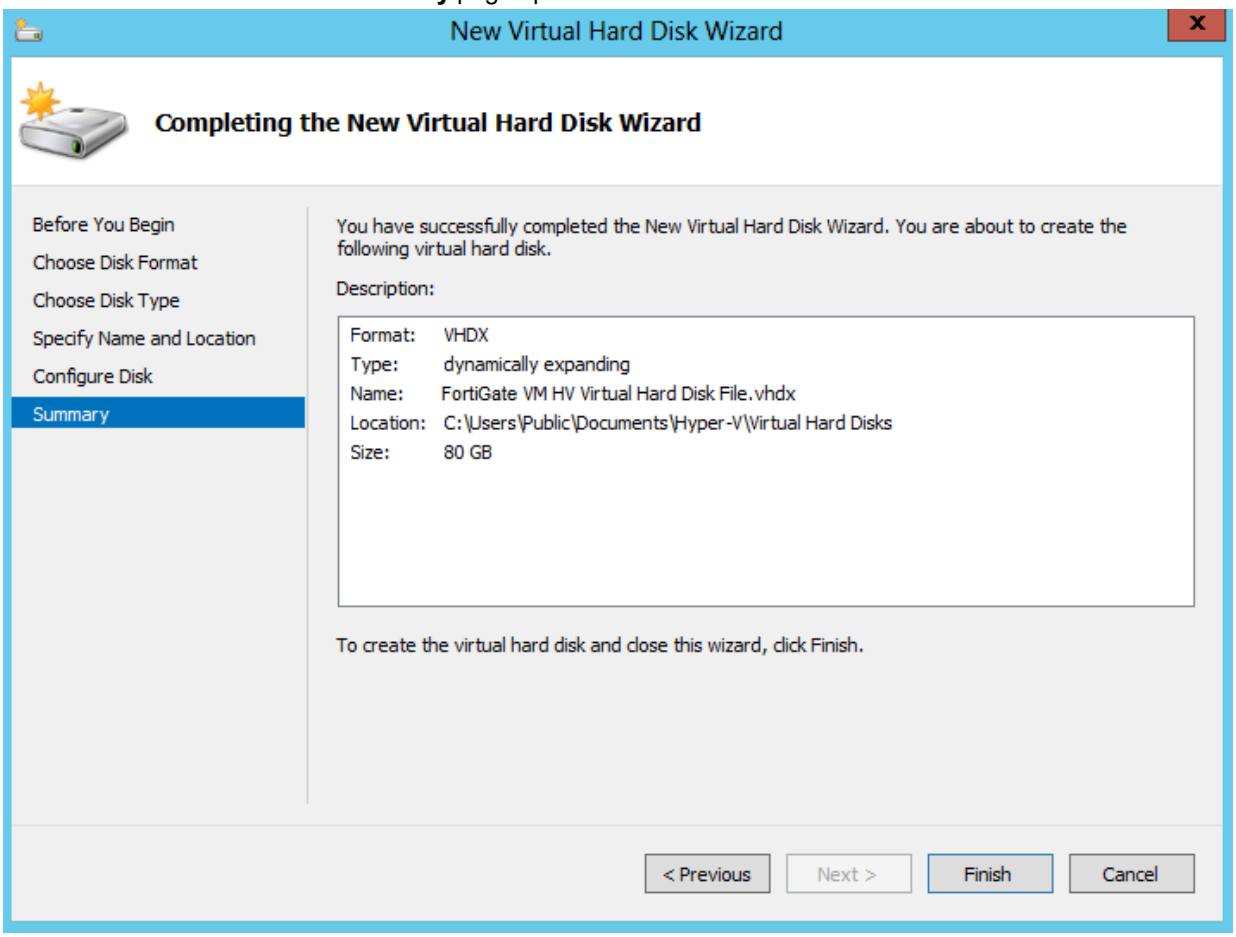
6. Specify the name and location of the virtual hard disk file. Use the **Browse** button to select a specific file folder on your server.

   Select **Next** to continue. The **Configure Disk** page opens.



7. Select to **Create a new blank virtual hard disk** and enter the size of the disk in GB. The maximum size is dependent on your server environment.

Select **Next** to continue. The **Summary** page opens.



8. The summary page provides details of the virtual hard disk. Select **Finish** to create the virtual hard disk.
9. Select **Apply** to save the settings and select **OK** to exit the settings page.

High Availability Hyper-V configuration

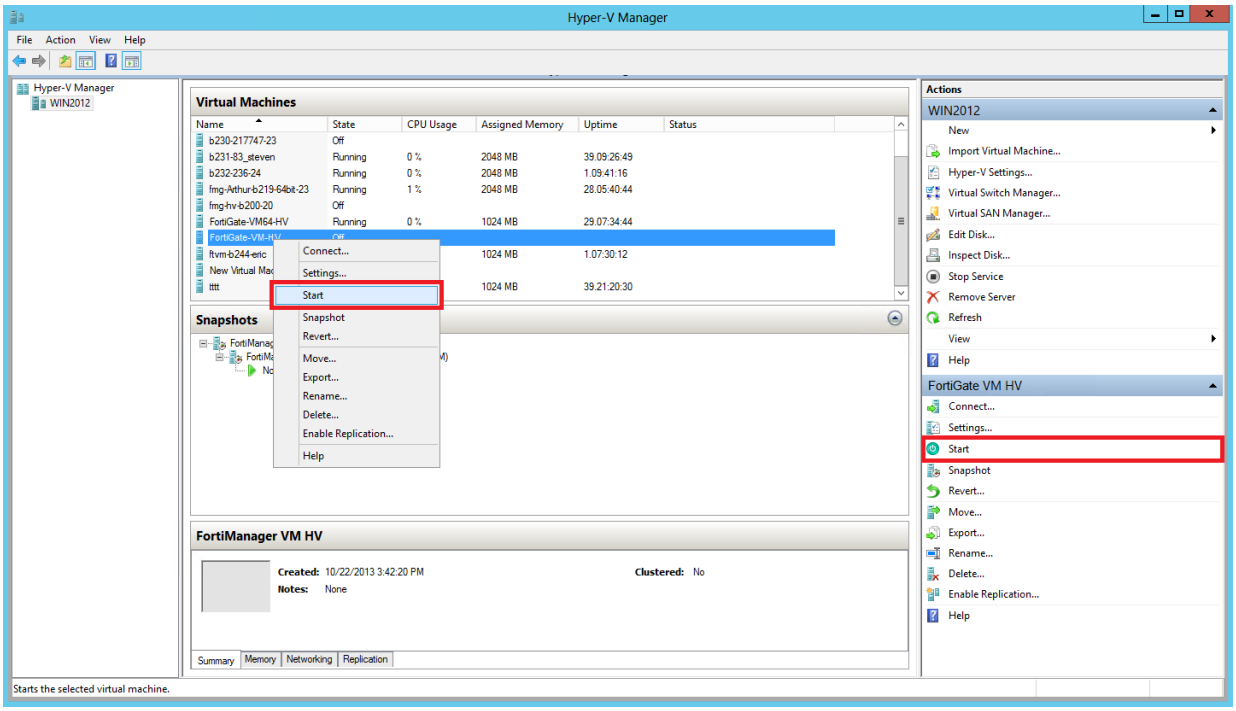
Promiscuous mode and support for MAC address spoofing is required for FortiGate-VM for Hyper-V to support FortiGate Clustering Protocol (FGCP) high availability (HA). By default the FortiGate-VM for Hyper-V has promiscuous mode enabled in the XML configuration file in the FortiGate-VM Hyper-V image. If you have problems with HA mode, confirm that this is still enabled.

In addition, because the FGCP applies virtual MAC addresses to FortiGate data interfaces and because these virtual MAC addresses mean that matching interfaces of different FortiGate-VM instances will have the same virtual MAC addresses you have to configure Hyper-V to allow MAC spoofing. But you should only enable MAC spoofing for FortiGate-VM data interfaces. You should not enable MAC spoofing for FortiGate HA heartbeat interfaces.

With promiscuous mode enabled and the correct MAC spoofing settings you should be able to configure HA between two or more FortiGate-VM for Hyper-V instances.

Start the FortiGate VM

You can now proceed to power on your FortiGate VM. Select the name of the FortiGate VM in the list of virtual machines, right-click, and select **Start** in the menu. Optionally, you can select the name of the FortiGate VM in the list of virtual machines and select **Start** in the **Actions** menu.



Deployment example – KVM

Once you have downloaded the FORTINET.out.kvm.zip file and extracted virtual hard drive image file fortios.qcow2, you can create the virtual machine in your KVM environment.

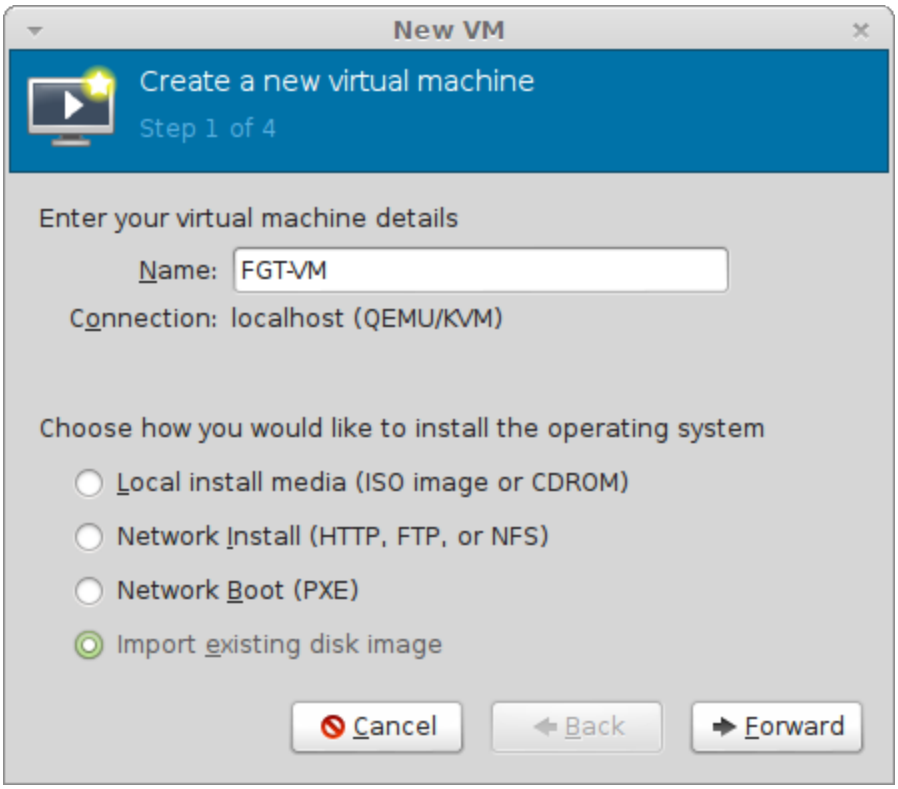
The following topics are included in this section:

Create the FortiGate VM virtual machine

To create the FortiGate VM virtual machine:

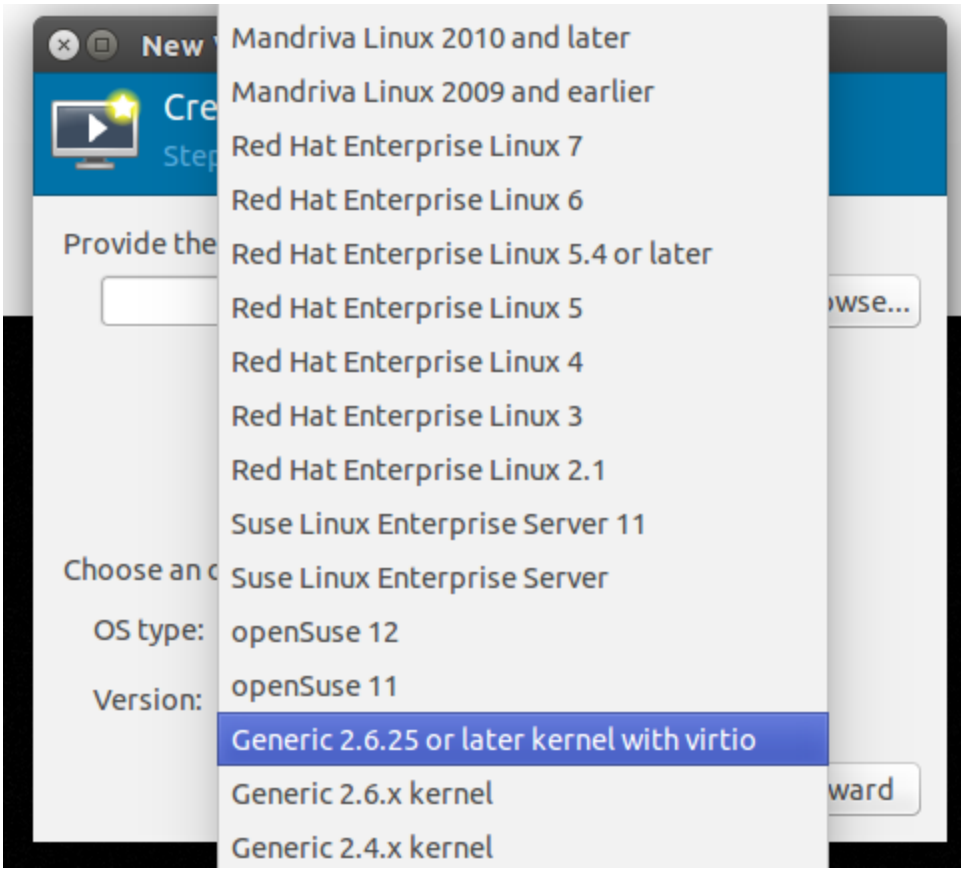
1. Launch Virtual Machine Manager (virt-manager) on your KVM host server.

   The **Virtual Machine Manager** home page opens.
2. In the toolbar, select **Create a new virtual machine**.



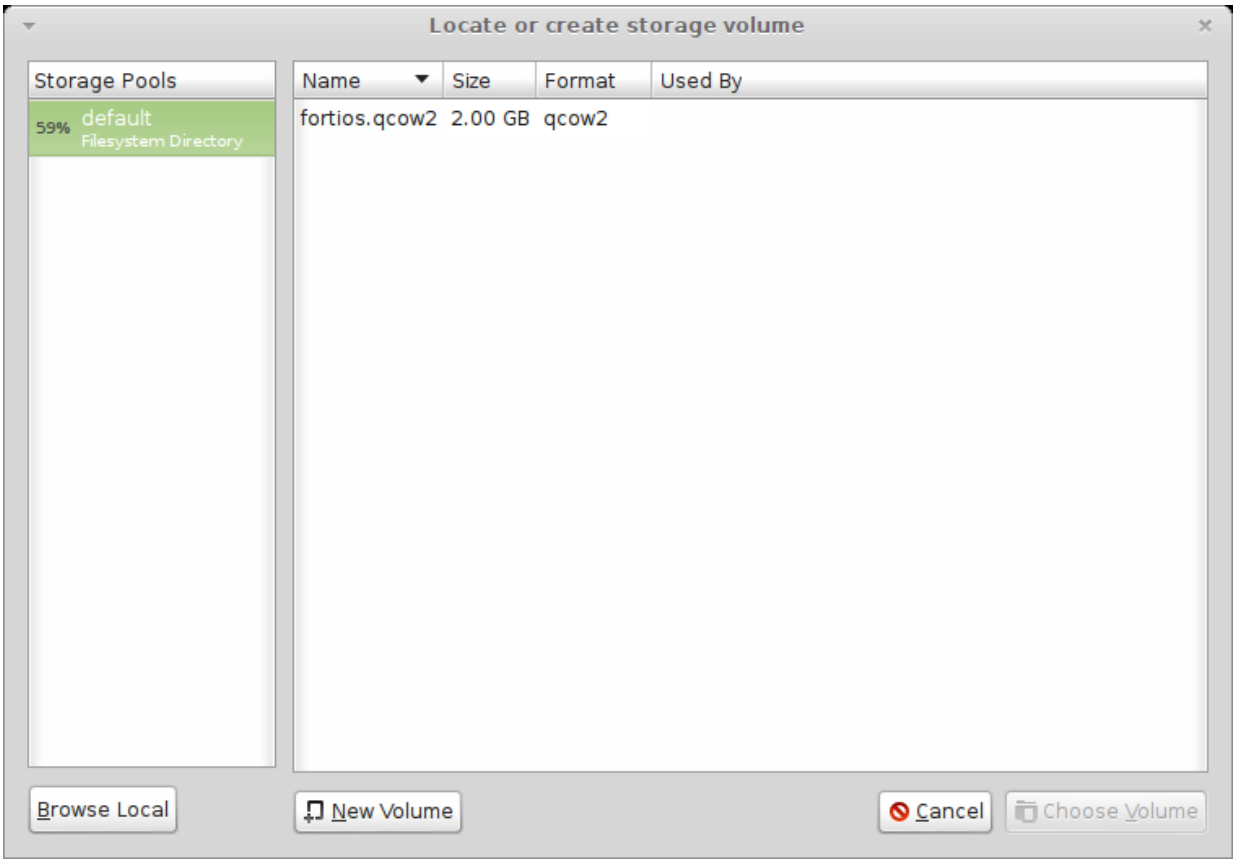
3. Enter a **Name** for the VM, FGT-VM for example.
4. Ensure that **Connection** is localhost. (This is the default.)
5. Select **Import existing disk image**.

6. Select **Forward**.



7. In **OS Type** select **Linux**.
8. In **Version**, select a Generic version with virtio.

9. Select **Browse**.



10. If you copied the fortios.qcow2 file to `/var/lib/libvirt/images`, it will be visible on the right. If you saved it somewhere else on your server, select Browse Local and find it.
11. Choose **Choose Volume**.
12. Select **Forward**.
13. Specify the amount of memory and number of CPUs to allocate to this virtual machine. The amounts must not exceed your license limits. See Virtual FortiOS Overview on page 11.
14. Select **Forward**.
15. Expand **Advanced options**. A new virtual machine includes one network adapter by default. Select a network adapter on the host computer. Optionally, set a specific MAC address for the virtual network interface. Set **Virt Type** to **virtio** and **Architecture** to **qcow2**.
16. Select **Finish**.

Configure FortiGate VM hardware settings

Before powering on your FortiGate VM you must add the log disk and configure the virtual hardware of your FortiGate VM.

To configure settings for FortiGate VM on the server:

1. In the Virtual Machine Manager, locate the name of the virtual machine and then select Open from the toolbar.
2. Select **Add Hardware**. In the **Add Hardware** window select **Storage**.

3. Select **Create a disk image on the computer's harddrive** and set the size to 30GB.

If you know your environment will expand in the future, it is recommended to increase the hard disk size beyond 30GB. The VM license limit is 2TB.

4. Enter:

Device type	Virtio disk
Cache mode	Default
Storage format	raw

Even though raw is the storage format listed, the qcow2 format is also supported.

5. Select **Network** to configure add more the network interfaces. The **Device type** must be **Virtio**.

   A new virtual machine includes one network adapter by default. You can add more through the Add Hardware window. FortiGate VM requires four network adapters. You can configure network adapters to connect to a virtual switch or to network adapters on the host computer.
6. Select **Finish**.

Start the FortiGate VM

You can now proceed to power on your FortiGate VM. Select the name of the FortiGate VM in the list of virtual machines. In the toolbar, select **Console** and then select **Start**.

Deployment example – OpenXen

Once you have downloaded the FORTINET.out.OpenXen.zip file and extracted virtual hard drive image file fortios.qcow2, you can create the virtual machine in your OpenXen environment.

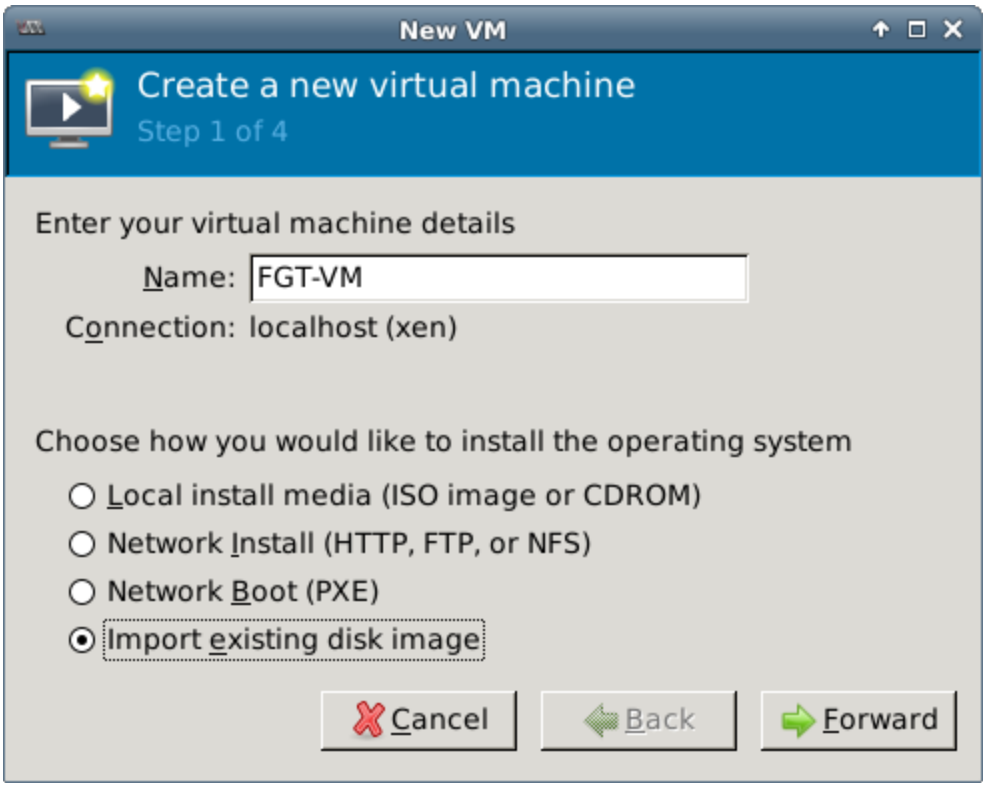
The following topics are included in this section:

Create the FortiGate VM virtual machine (VMM)

To create the FortiGate VM virtual machine:

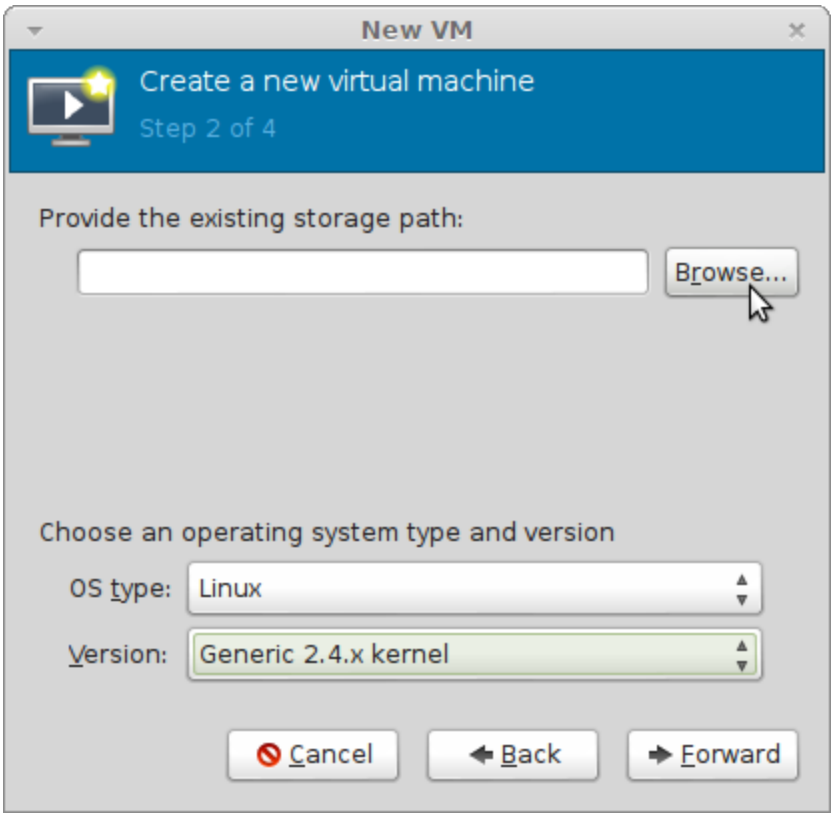
1. Launch Virtual Machine Manager (virt-manager) on your OpenXen host server.

   The **Virtual Machine Manager** home page opens.
2. In the toolbar, select **Create a new virtual machine**.



3. Enter a **Name** for the VM, FGT-VM for example.
4. Ensure that **Connection** is localhost. (This is the default.)
5. Select **Import existing disk image**.

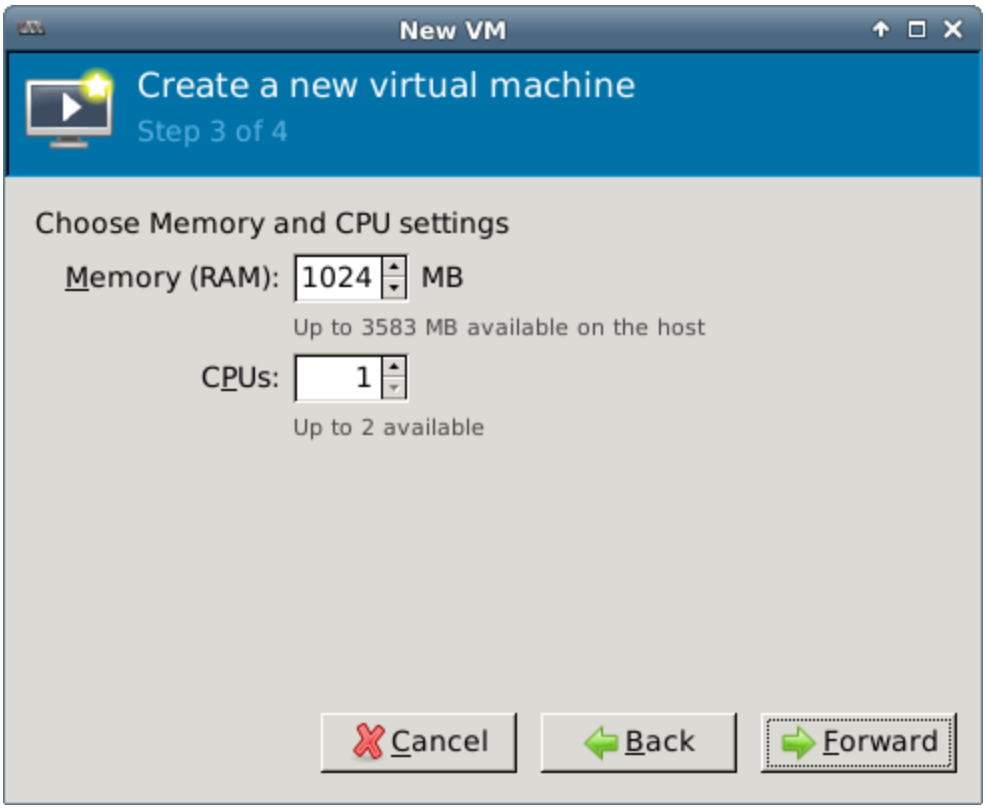
6. Select **Forward**.



7. In **OS Type** select **Linux**.
8. In **Version**, select **Generic 2.4.x.kernel**.
9. Select **Browse**.

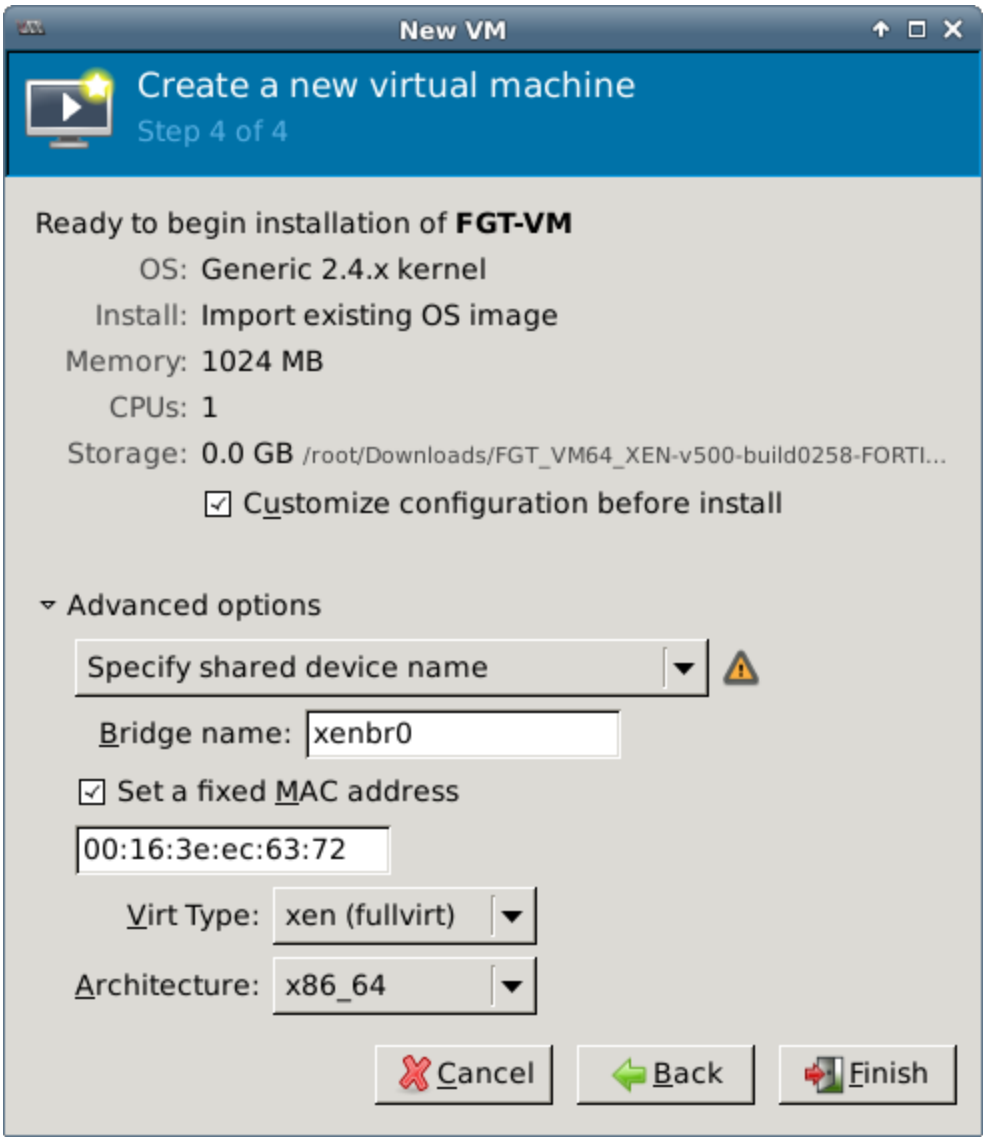
   The **Locate or create storage volume** window opens.
10. Select **Browse Local,** find the fortios.qcow2 disk image file.
11. Select fortios.qcow2 and select **Choose Volume**.

12. Select **Forward**.



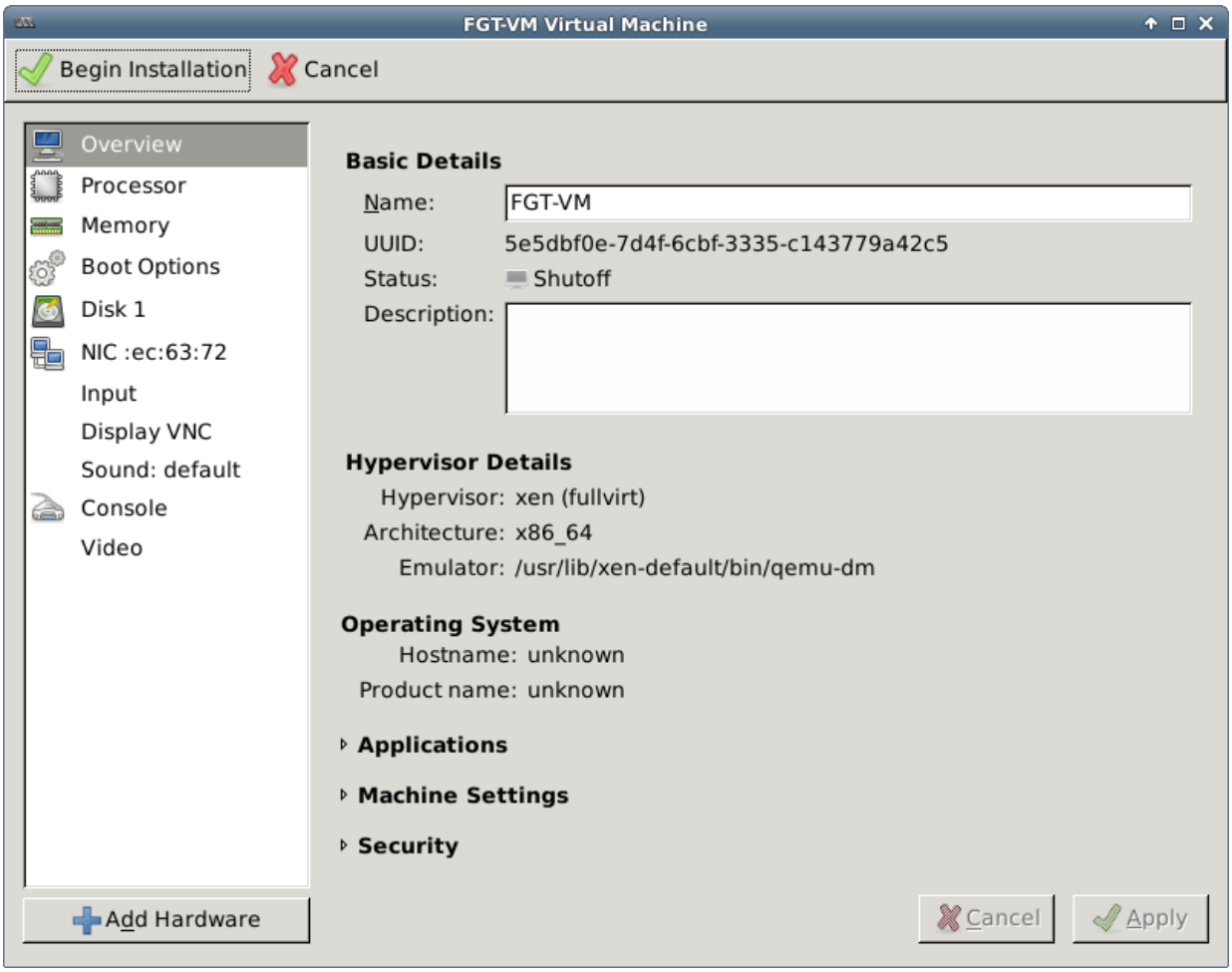
13. Specify the amount of memory and number of CPUs to allocate to this virtual machine. The amounts must not exceed your license limits.

14. Select **Forward**.



15. Select **Customize configuration before install**. This enables you to make some hardware configuration changes before VM creation is started.
16. Expand **Advanced options**. A new virtual machine includes one network adapter by default. Select **Specify shared device name** and enter the name of the bridge interface on the OpenXen host. Optionally, set a specific MAC address for the virtual network interface. **Virt Type** and **Architecture** are set by default and should be correct.
17. Select **Finish**.

    The virtual machine hardware configuration window opens.



You can use this window to add hardware such as network interfaces and disk drives.

18. Select **Add Hardware**. In the **Add Hardware** window select **Storage**.
19. Select **Create a disk image on the computer's harddrive** and set the size to 30GB.

If you know your environment will expand in the future, it is recommended to increase the hard disk size beyond 30GB. The VM license limit is 2TB.

20. Enter:

Device type	Virtio disk
Cache mode	Default
Storage format	raw

21. Select **Network** to configure add more the network interfaces. The **Device type** must be **Virtio**.

    A new virtual machine includes one network adapter by default. You can add more through the Add Hardware window. FortiGate VM requires four network adapters. You can configure network adapters to connect to a virtual

switch or to network adapters on the host computer.

22. Select **Finish**.
23. Select **Begin Installation**. After the installation completes successfully, the VM starts and the console window opens.

Deployment example – Citrix XenServer

Once you have downloaded the FORTINET.out.CitrixXen.zip file and extracted the files, you can create the virtual machine in your Citrix Xen environment.

The following topics are included in this section:

Create the FortiGate VM virtual machine (XenCenter)

To create the FortiGate VM virtual machine from the OVF file

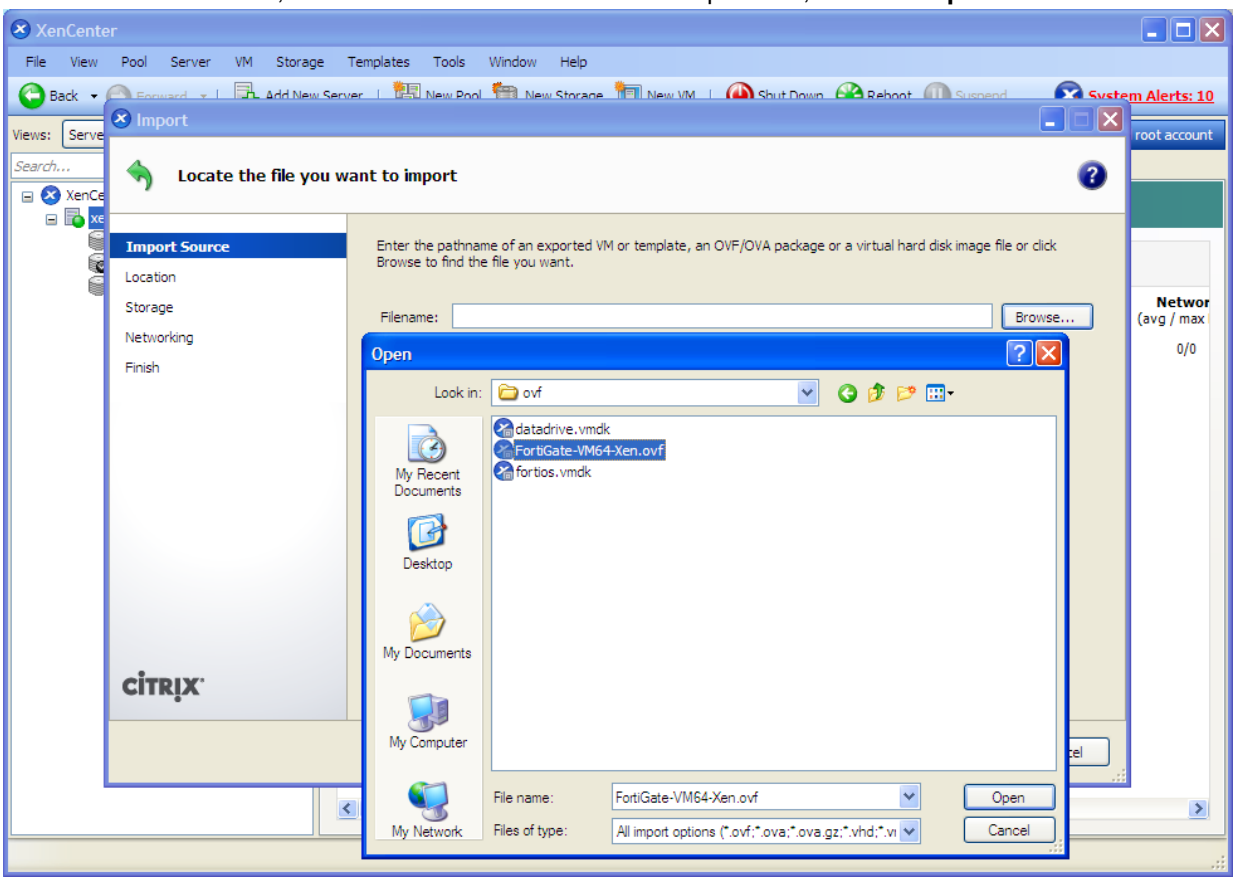
1. Launch XenCenter on your management computer.

   The management computer can be any computer that can run Citrix XenCenter, a Windows application.
2. If you have not already done so, select **ADD a server**. Enter your Citrix XenServer IP address and the root logon credentials required to manage that server.

   Your Citrix XenServer is added to the list in the left pane.

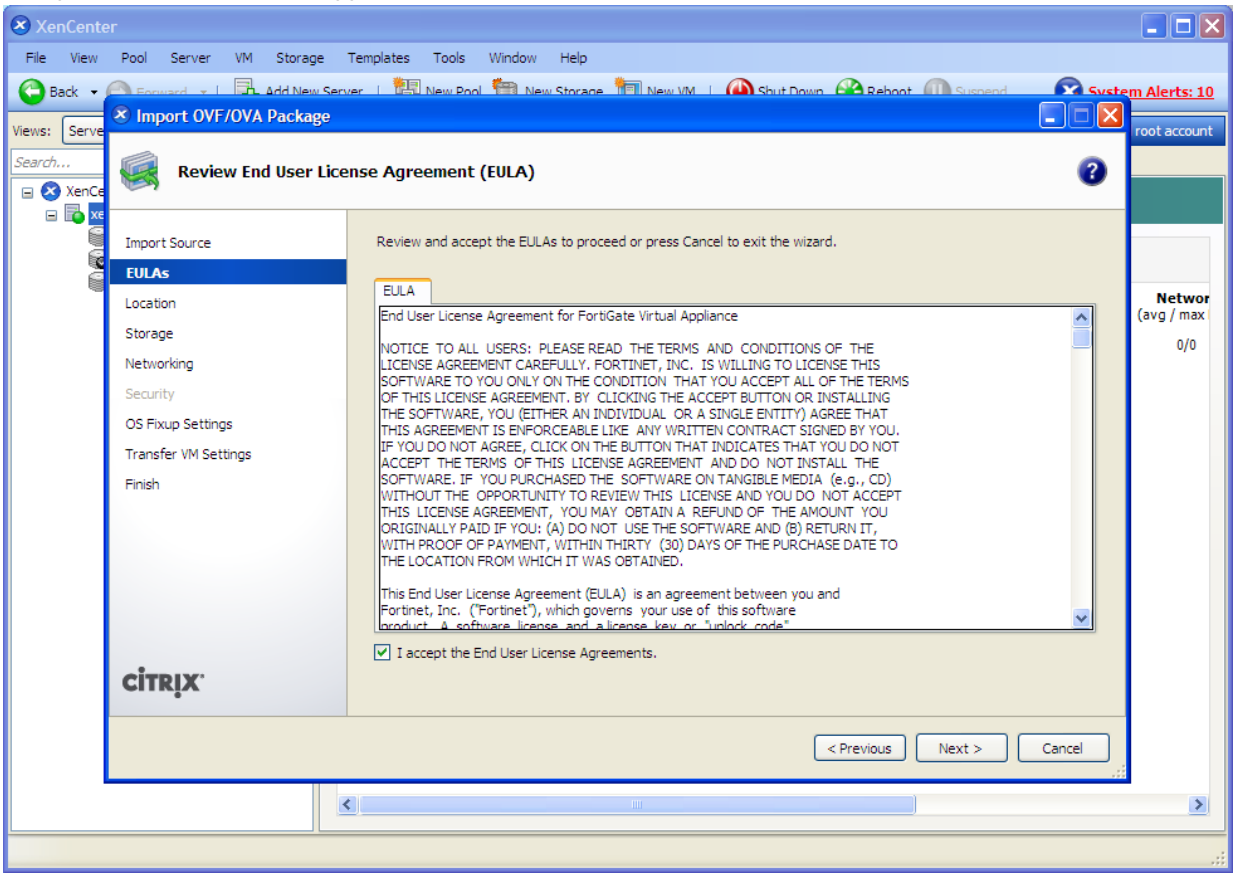
   The **Virtual Machine Manager** home page opens.
3. Go to **File > Import**. An import dialog will appear.

4. Click the **Browse** button, find the FortiGate-VM64-Xen.ovf template file, then click **Open**.



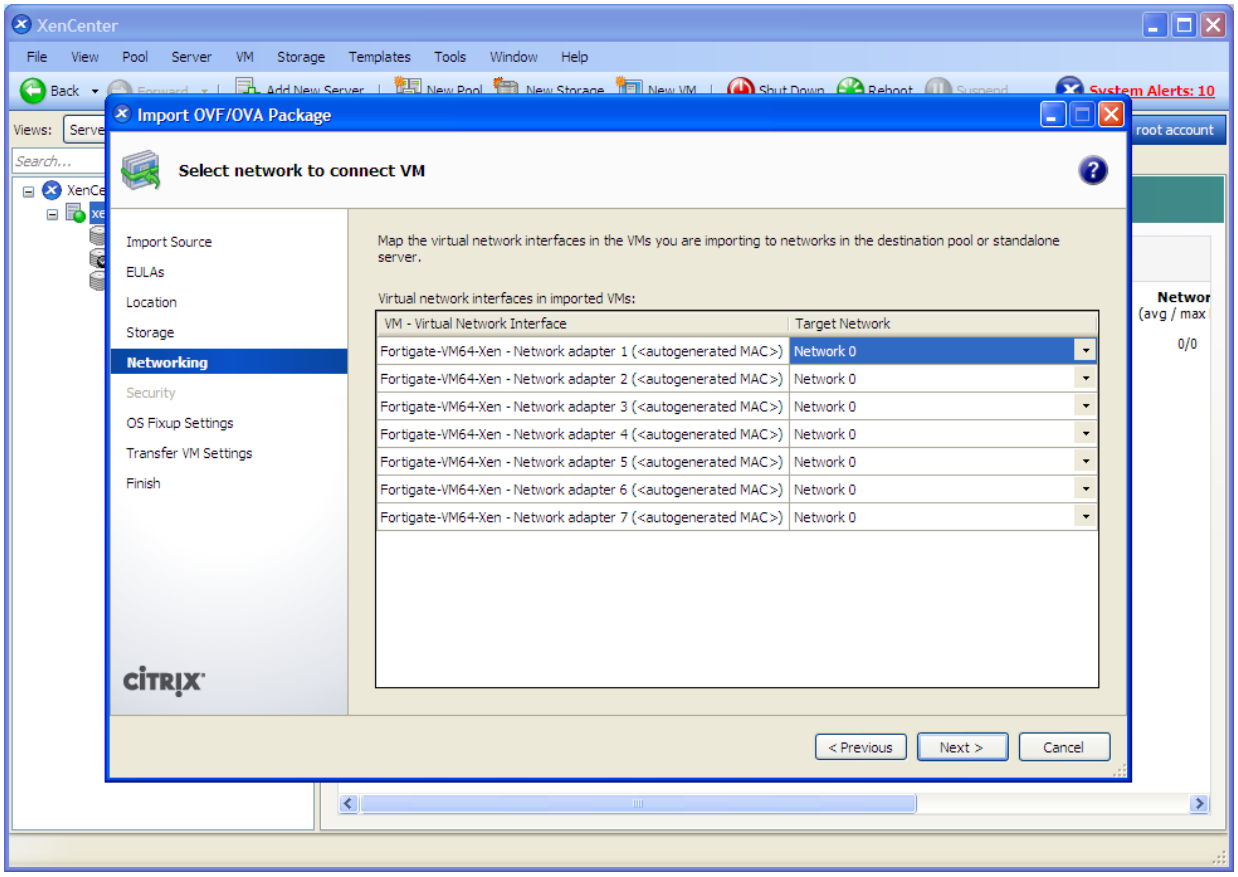
5. Select **Next**.

6. Accept the FortiGate Virtual Appliance EULA, then select **Next**.



7. Choose the pool or standalone server that will host the VM, then select **Next**.
8. Select the storage location for FortiGate VM disk drives or accept the default. Select **Next**.

9. Configure how each vNIC (virtual network adapter) in FortiGate VM will be mapped to each vNetwork on the Citrix XenServer, then click **Next**.



10. Click **Next** to skip OS fixup.
11. Select **Next** to use the default network settings for transferring the VM to the host.
12. Select **Finish**.

The Citrix XenServer imports the FortiGate VM files and configures the VM as specified in the OVF template. Depending on your computer's hardware speed and resource load, and also on the file size and speed of the network connection, this might take several minutes to complete.

When VM import is complete, the XenCenter left pane includes the FortiGate VM in the list of deployed VMs for your Citrix XenServer.

Configure virtual hardware

Before you start your FortiGate-VM for the first time, you need to adjust your virtual machine's virtual hardware settings to meet your network requirements.

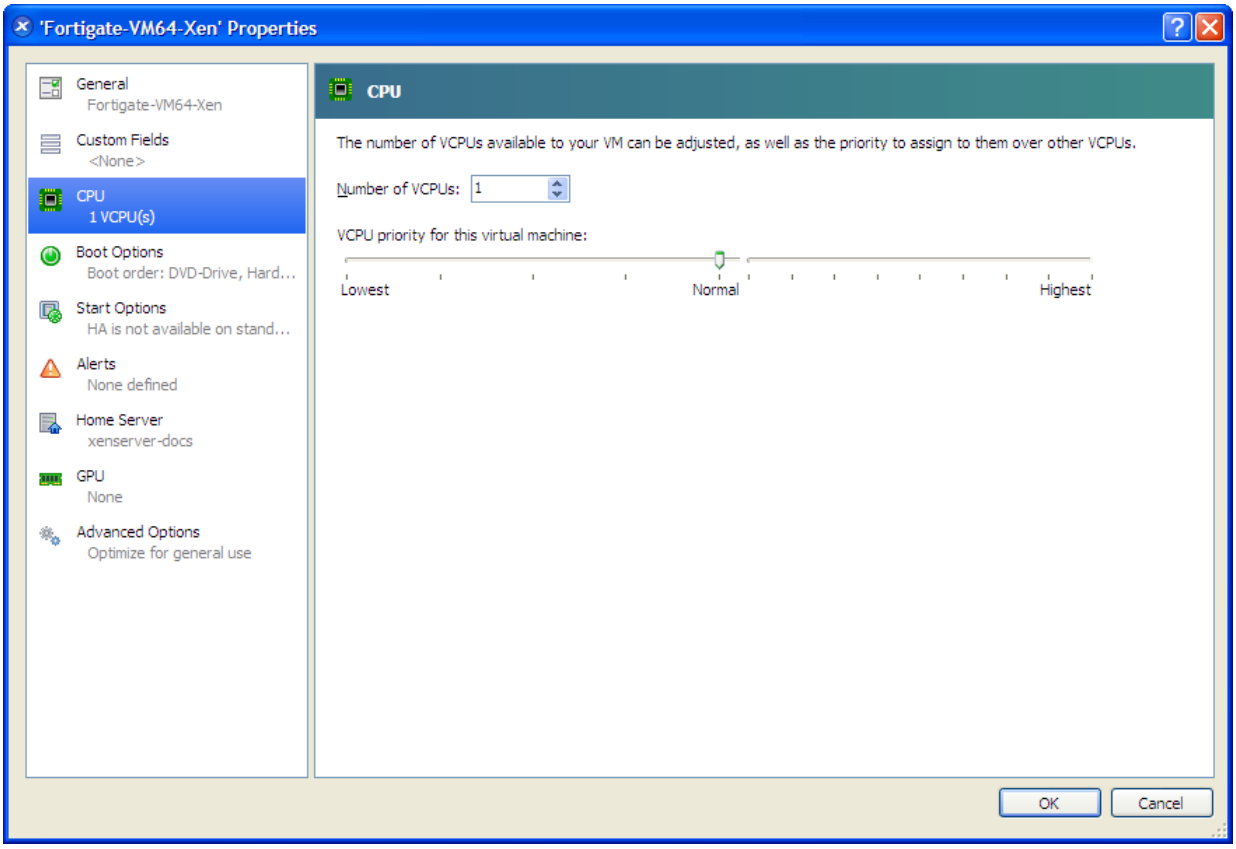
Configuring number of CPUs and memory size

Your FortiGate-VM license limits the number CPUs and amount of memory that you can use. The amounts you allocate must not exceed your license limits.

To access virtual machine settings

1. Open XenCenter.
2. Select your FortiGate VM in the left pane.
   The tabs in the right pane provide access to the virtual hardware configuration. The Console tab provides access to the FortiGate console.

1. To set the number of CPUs
2. In the XenCenter left pane, right-click the FortiGate VM and select Properties.
   The Properties window opens.
3. In the left pane, select CPU.

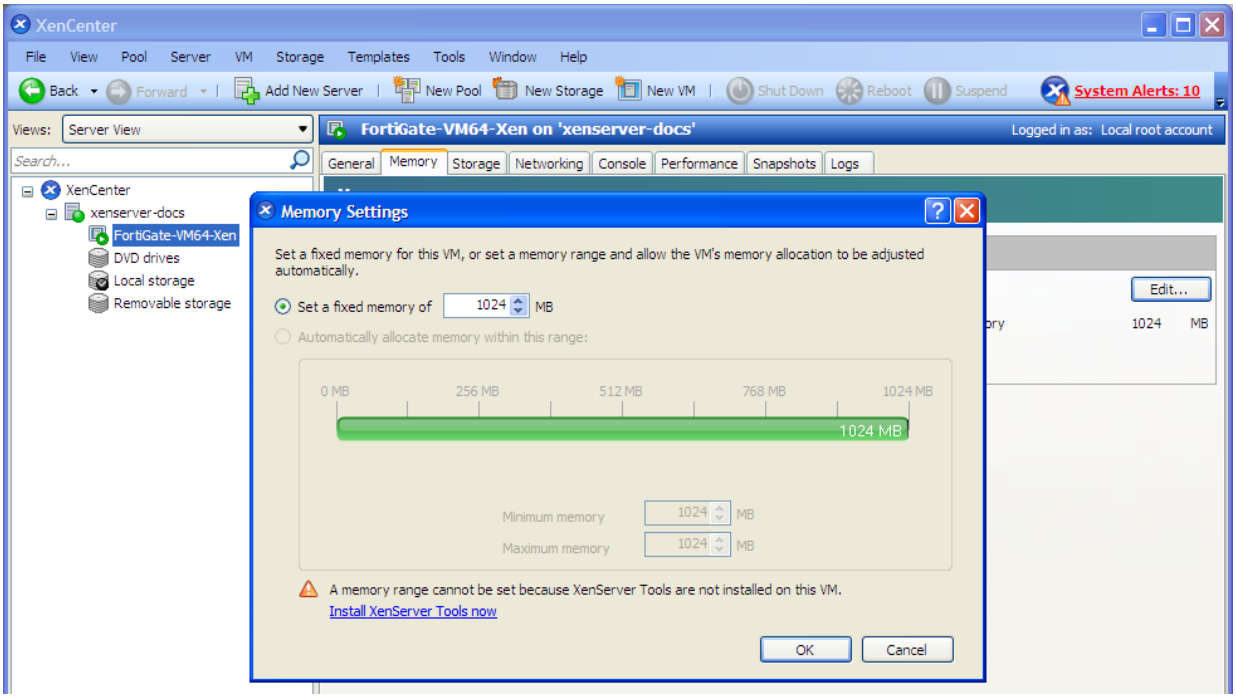


4. Adjust **Number of CPUs** and then select **OK**.

XenCenter will warn if you select more CPUs than the Xen host computer contains. Such a configuration might reduce performance.

To set memory size

1. In the XenCenter left pane, select the FortiGate VM.
2. In the right pane, select the **Memory** tab.
3. Select **Edit**, modify the value in the **Set a fixed memory of** field and select **OK**.



Configuring disk storage

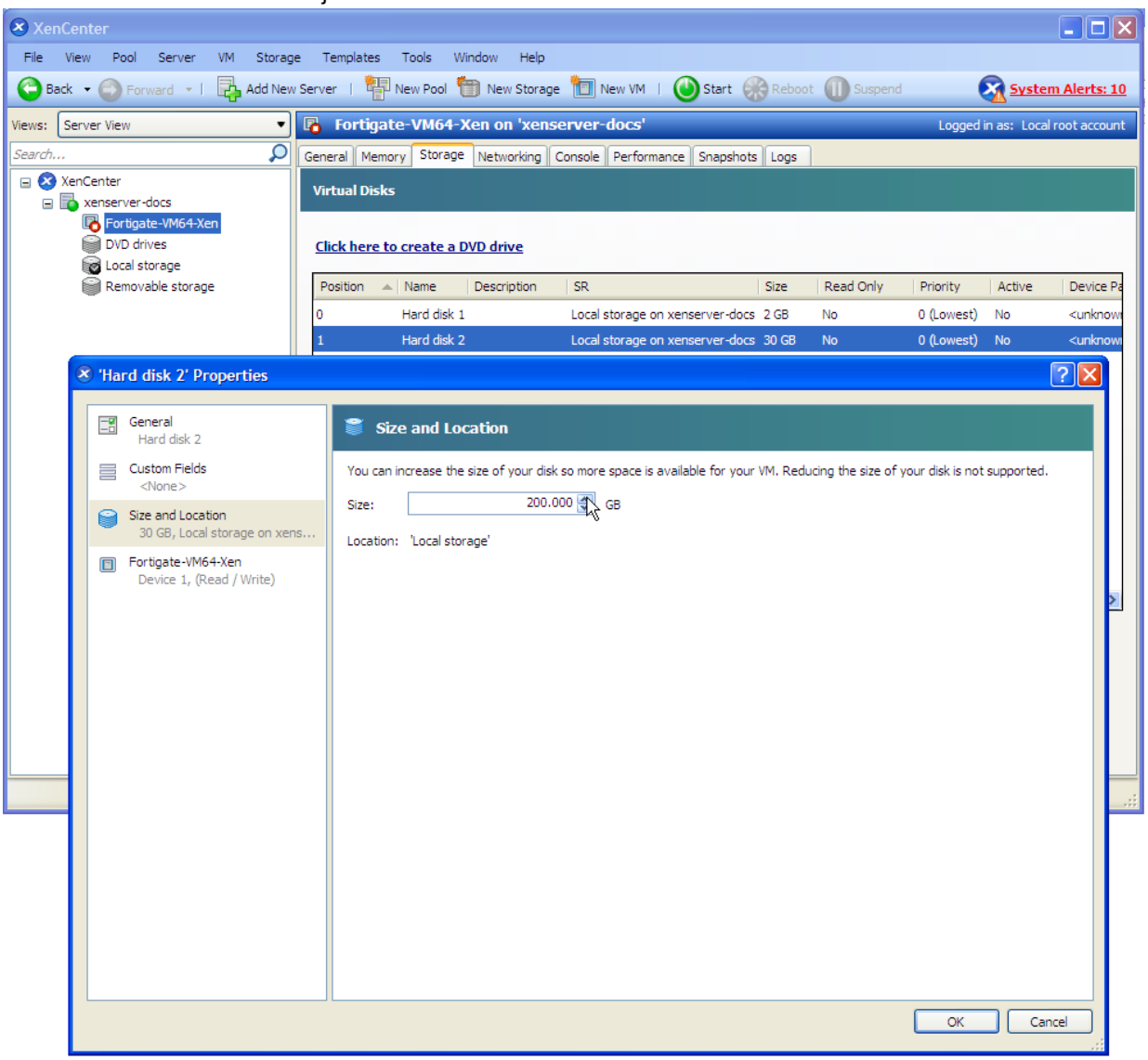
By default the FortiGate VM data disk 30GB. You will probably want to increase this. Disk resizing must be done before you start the VM for the first time.

To resize the FortiGate data disk

1. In the XenCenter left pane, select the FortiGate VM.
2. Select the **Storage** tab. Select **Hard disk 2** (the 30GB drive), then select **Properties**.

   The **'Hard disk 2' Properties** window opens.

3. Select **Size and Location**. Adjust **Size** and select **OK**.



FortiGate VM Initial Configuration

Before you can connect to the FortiGate VM web-based manager you must configure a network interface in the FortiGate VM console. Once an interface with administrative access is configured, you can connect to the FortiGate VM web-based Manager and upload the FortiGate VM license file that you downloaded from the Customer Service & Support website.

The following topics are included in this section:

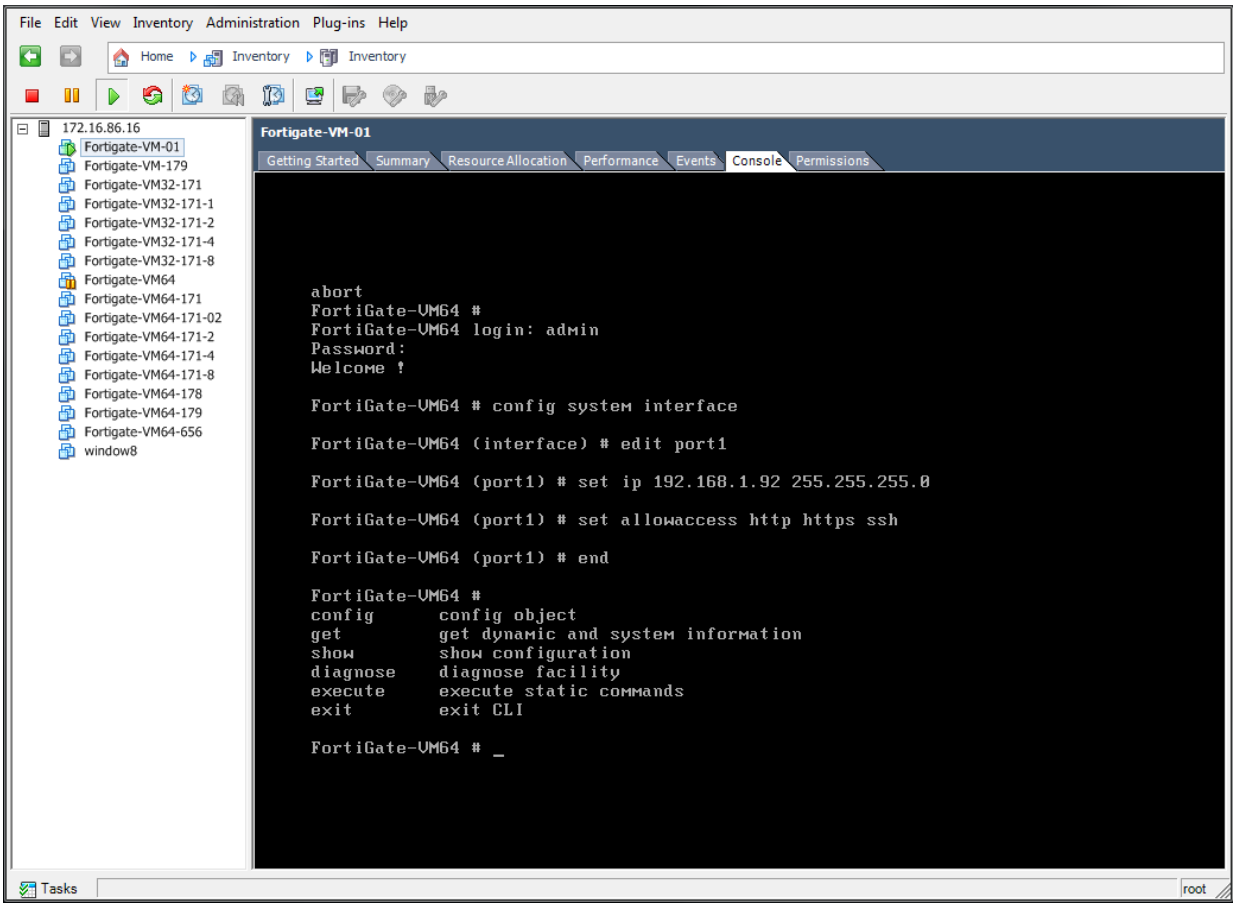
Set FortiGate VM port1 IP address

Hypervisor management environments include a guest console window. On the FortiGate VM, this provides access to the FortiGate console, equivalent to the console port on a hardware FortiGate unit. Before you can access the Web-based manager, you must configure FortiGate VM port1 with an IP address and administrative access.

To configure the port1 IP address:

1. In your hypervisor manager, start the FortiGate VM and access the console window.
   You might need to press Return to see a login prompt.

   Example of FortiGate VM console access:



2. At the FortiGate VM login prompt enter the username `admin`. By default there is no password. Just press Return.
3. Using CLI commands, configure the port1 IP address and netmask. Also, HTTP access must be enabled because until it is licensed the FortiGate VM supports only low-strength encryption. HTTPS access will not work.

   For example:

```
config system interface
   edit port1
      set ip 192.168.0.100 255.255.255.0
      append allowaccess http
   end
```

You can also use the `append allowaccess` CLI command to enable other access protocols, such as `auto-ipsec`, `http`, `probe-response`, `radius-acct`, `snmp`, and `telnet`. The `ping`, `https`, `ssh`, and `fgfm` protocols are enabled on the `port1` interface by default.

4. To configure the default gateway, enter the following CLI commands:

```
config router static
   edit 1
      set device port1
      set gateway <class_ip>
end
```

You must configure the default gateway with an IPv4 address. FortiGate VM needs to access the Internet to contact the FortiGuard Distribution Network (FDN) to validate its license.

5. To configure your DNS servers, enter the following CLI commands:

```
config system dns
   set primary <Primary DNS server>
   set secondary <Secondary DNS server>
end
```

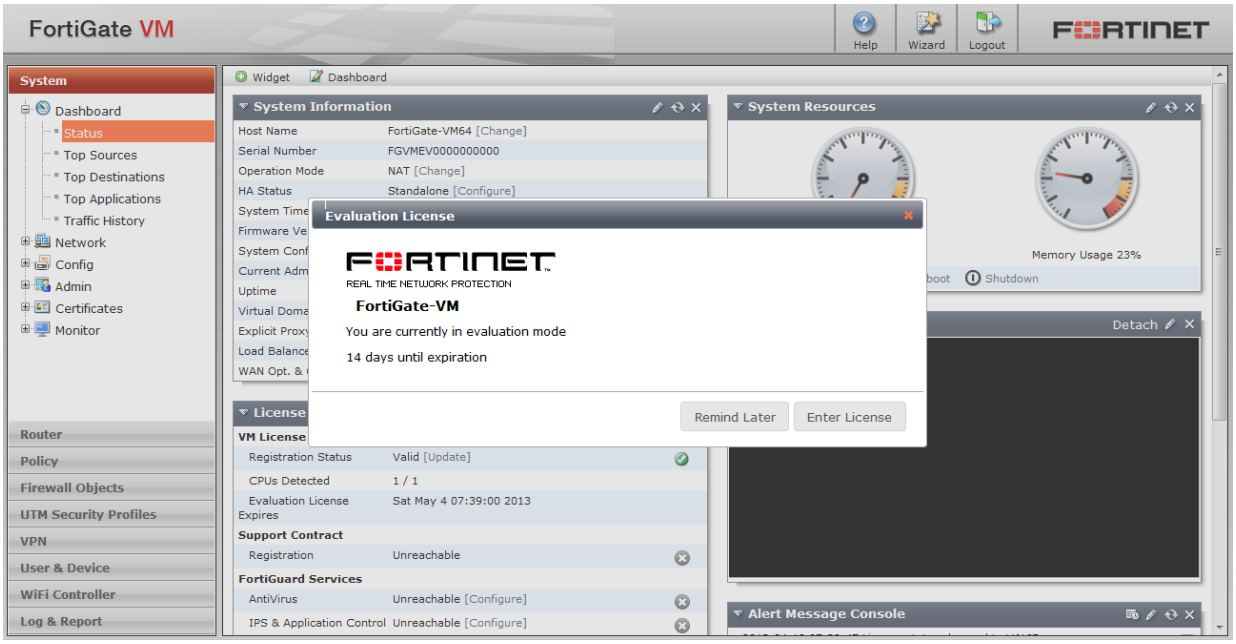
The default DNS servers are `208.91.112.53` and `208.91.112.52`.

6. To upload the FortiGate VM license from an FTP or TFTP server, use the following CLI command:

```
execute restore vmlicense {ftp | tftp} <VM license file name> <Server IP or FQDN>
    [:server port]
```

You can also upload the license in the FortiGate VM Web-based Manager. See Set FortiGate VM port1 IP address on page 70.

Web-based Manager and Evaluation License dialog box



Connect to the FortiGate VM Web-based Manager

When you have configured the port1 IP address and netmask, launch a web browser and enter the IP address that you configured for port1. At the login page, enter the username `admin` and password field and select **Login**. The default password is no password. The Web-based Manager will appear with an **Evaluation License** dialog box.

Due to low encryption on the FortiGate side of the connection, some modern browsers will not allow the connection. If that is the case, the adjusting of the browser settings is unlikely to make a difference. There are two options:

- Use FTP or TFTP to apply the license
- Make sure that the interface on the port being accessed has been configured to allow HTTP/HTTPS access

Upload the FortiGate VM license file

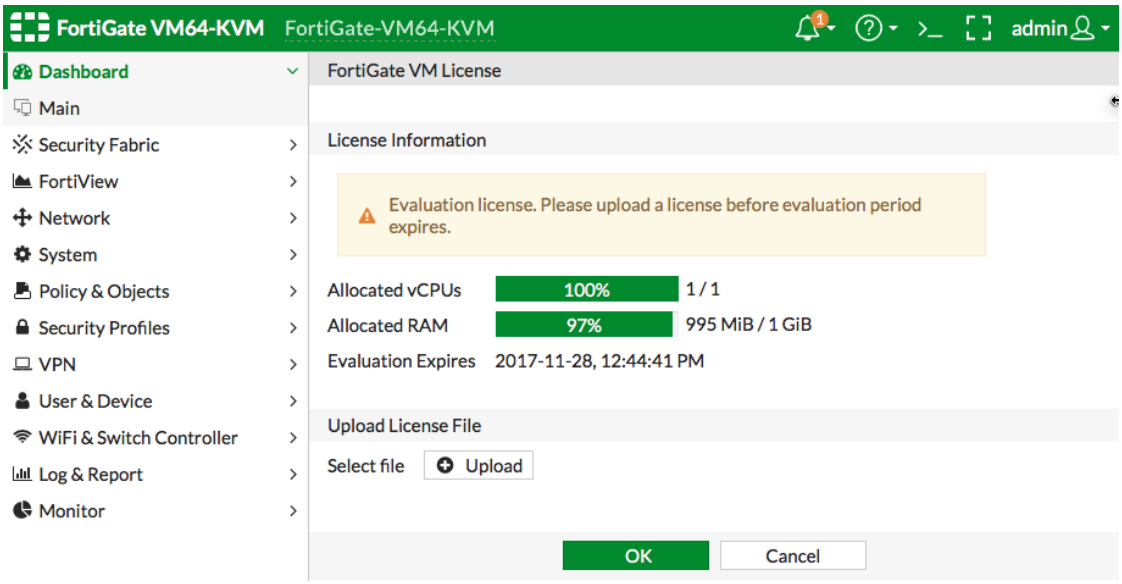
Every Fortinet VM includes a 15-day trial license. During this time the FortiGate VM operates in evaluation mode. Before using the FortiGate VM you must enter the license file that you downloaded from the Customer Service & Support website upon registration.

GUI

To upload the FortiGate VM licence file:

1. There are 2 ways to get to the License upload window.
   i. In the **Dashboard > Main** window, in the **Virtual Machine** widget, left click on the **FGVMEV** (FortiGate-VM Evaluation) **License** icon. This will reveal a menu of selections to take you to directly to the **FortiGate VM License** window or to the **FortiGuard Details** window.
   ii. Go to **System > FortiGuard**. In the **Licence Information** section, go to the **Virtual Machine** row and click on the link to **FortiGate VM License**.
2. In the **Evaluation License** dialog box, select **Enter License**.
   The license upload page opens.

   License upload page:



3. Select **Upload** and locate the license file (`.lic`) on your computer. Select **OK** to upload the license file.
4. Refresh the browser to login.
5. Enter `admin` in the Name field and select **Login**. The VM registration status appears as valid in the License Information widget once the license has been validated by the FortiGuard Distribution Network (FDN) or FortiManager for closed networks.

Modern browsers can have an issue with allowing connecting to a FortiGate if the encryption on the device is too low. Adjusting browser settings does not normally mitigate the issue. If this happens, Admins must use a FTP/TFTP server to apply the license.

CLI

You can also upload the license file via the CLI using the following CLI command:

```
execute restore vmlicense [ftp | tftp] <filenmame string> <ftp server>[:ftp port]
```

Example:

The following is an example output when using a tftp server to install license.

```
exec restore vmlicense tftp license.lic 10.0.1.2
This operation will overwrite the current VM license!Do you want to continue? (y/n)y
Please wait...Connect to tftp server 10.0.1.2 ...
Get VM license from tftp server OK.
VM license install succeeded.
Rebooting firewall.
```

The command has the side effect of rebooting the firewall without giving you a chance to back out or delay the reboot, so becareful about the timing of using the command.

Validate the FortiGate VM license with FortiManager

You can validate your FortiGate VM license with some models of FortiManager. To determine whether your FortiManager unit has the VM Activation feature, see Features section of the FortiManager Product Data sheet.

To validate your FortiGate VM with your FortiManager:

1. To configure your FortiManager as a closed network, enter the following CLI command on your FortiManager:
```
config fmupdate publicnetwork
   set status disable
   end
```
2. To configure FortiGate VM to use FortiManager as its override server, enter the following CLI commands on your FortiGate VM:
```
config system central-management
   set mode normal
   set type fortimanager
   set fmg <IPv4 address of the FortiManager device>
   set fmg-source-ip <Source IPv4 address when connecting to the FortiManager device>
   set include-default-servers disable
   set vdom <Enter the name of the VDOM to use when communicating with the FortiManager
       device>
   end
```
3. Load the FortiGate VM license file in the Web-based Manager. Go to **System > Dashboard > Status**. In the **License Information** widget, in the **Registration Status** field, select **Update**. Browse for the `.lic` license file and select **OK**.
4. To activate the FortiGate VM license, enter the following CLI command on your FortiGate VM:
```
execute update-now
```
5. To check the FortiGate VM license status, enter the following CLI commands on your FortiGate VM:
```
get system status
```

The following output is displayed:

```
Version: Fortigate-VM v5.0,build0099,120910 (Interim)
Virus-DB: 15.00361(2011-08-24 17:17)
Extended DB: 15.00000(2011-08-24 17:09)
Extreme DB: 14.00000(2011-08-24 17:10)
IPS-DB: 3.00224(2011-10-28 16:39)
FortiClient application signature package: 1.456(2012-01-17 18:27)
Serial-Number: FGVM02Q105060000
License Status: Valid
BIOS version: 04000002
Log hard disk: Available
Hostname: Fortigate-VM
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Distribution: International
```

```
Branch point: 511
Release Version Information: MR3 Patch 4
System time: Wed Jan 18 11:24:34 2012

diagnose hardware sysinfo vm full
   The following output is displayed:
UUID: 564db33a29519f6b1025bf8539a41e92
valid: 1
status: 1
code: 200 (If the license is a duplicate, code 401 will be displayed)
warn: 0
copy: 0
received: 45438
warning: 0
recv: 201201201918
dup:
```

Licensing timeout

In closed environments without Internet access, it is mandatory to perform offline licensing of the virtual FortiGate using a FortiManager as a license server. If the FortiGate-VM cannot perform license validation within the license timeout period, which is 30 days, the FortiGate will discard all packets and effectively ceasing operation as a firewall.

The status of the licence will go through some status changes before it times out.

Status	Description
Valid	The FortiGate can connect and validate against a FortiManager or FDS
Warning	The FortiGate ***cannot*** connect and validate against a FortiManager or FDS. A check is made against how many days the Warning status has been continuous. If the number is less the 30 days the status does not change.
Invalid	The FortiGate ***cannot*** connect and validate against a FortiManager or FDS. A check is made against how many days the Warning status has been continuous. If the number is 30 days or more, the status changes to Invalid.The firewall ceases to function properly.

There is only a single log entry after the virtual FortiGate cannot access the license server for the license expiration period. This means that when you go searching the logs for a reason for the FortiGate being offline there will not be a long list of error logs that draw attention to the issue. There will only be the one entry.

Configure your FortiGate VM

Once the FortiGate VM license has been validated you can begin to configure your device. You can use the **Wizard** located in the top toolbar for basic configuration including enabling central management, setting the admin password, setting the time zone, and port configuration.

For more information on configuring your FortiGate VM see the FortiOS Handbook at http://docs.fortinet.com.